# AREA CODE CHANGE

**Please note that the area code for Paradyne Corporation in Largo, Florida has changed from 813 to 727.**

**For any Paradyne telephone number that appears in this manual with an 813 area code, dial 727 instead.**

# HOTWIRE DIGITAL SUBSCRIBER LINE ACCESS MULTIPLEXER (DSLAM)

## NETWORK CONFIGURATION GUIDE

**Document No. 8000-A2-GB21-10**

PARADYNE™

## Notice



## Warranty, Sales, and Service Information

Contact your sales or service representative directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, or training, use one of the following methods:

- **Via the Internet:** Visit the Paradyne World Wide Web site at http://www.paradyne.com
- **Via Telephone:** Call our automated call system to receive current information via fax or to speak with a company representative.
  - — Within the U.S.A., call 1-800-870-2221
  - — International, call 813-530-2340

## Trademarks



Printed on recycled paper

# Contents


## About This Guide

- Document Purpose and Intended Audience . . . . . v
- Document Summary . . . . . vi
- Product-Related Documents . . . . . vii

## 1 Introduction to the HotWire DSLAM

- What is the HotWire DSLAM? . . . . . 1-1
- HotWire DSLAM Components . . . . . 1-2
  - HotWire DSLAM Chassis . . . . . 1-2
  - MCC Card . . . . . 1-4
  - DSL Cards . . . . . 1-4
- What is the HotWire 5446 RTU? . . . . . 1-5
- Overview of the HotWire DSLAM Network Model . . . . . 1-7
- Understanding the Domain Types . . . . . 1-11

## 2 Customer Domain Features

- Overview . . . . . 2-1
- Data Rates . . . . . 2-1
- Protocols . . . . . 2-2
- Proxy ARP (Theory of Operation) . . . . . 2-3
  - Scenario 1: Without Proxy ARP . . . . . 2-3
  - Scenario 2: With Proxy ARP . . . . . 2-4
- Filtering . . . . . 2-5

## 3 Management Domain Features

- Overview . . . . . 3-1
- Network Management Systems — SNMP and DCE Manager . . . . . 3-1
- Applications for Management . . . . . 3-2
  - Ping . . . . . 3-2
  - tFTP Client . . . . . 3-3
  - Telnet . . . . . 3-3

## 4 Components of the Network Model


- Overview . . . . . 4-1
- Customer Domain Components . . . . . 4-1
  - Proxy ARP . . . . . 4-3
- Management Domain Components . . . . . 4-5
  - Discovering Devices on the Network (Discovery) . . . . . 4-6
  - MCC Card Proxy ARP . . . . . 4-7


## 5 IP Address Allocation


- Overview . . . . . 5-1
- Port Naming Convention . . . . . 5-1
- Assigning IP Addresses . . . . . 5-2
  - Host Addressing . . . . . 5-2
  - Structured Subnet Addressing . . . . . 5-3
- Management IP Address Allocation . . . . . 5-6
  - Peer IP Addresses . . . . . 5-7
- Customer IP Address Allocation . . . . . 5-9
- Recording Your Configuration Settings . . . . . 5-10


## 6 IP Routing


- Overview . . . . . 6-1
- Static Routes . . . . . 6-1
  - MCC Card Static Route Example . . . . . 6-3
  - DSL Card Static Route Example . . . . . 6-4
- Source-Based Routing . . . . . 6-5
  - Without Source-Based Routing . . . . . 6-5
  - With Source-Based Routing . . . . . 6-5


## 7 IP Filtering


- Overview . . . . . 7-1
- What is a Filter? . . . . . 7-1
- Security Advantages . . . . . 7-3
  - Management Traffic Leakage . . . . . 7-3
  - Service Security . . . . . 7-3
- Service Security Filtering Scenario . . . . . 7-4

## 8 SNMP Agent

- Overview . . . . . 8-1
- MIB Compliance . . . . . 8-1
- Supported Traps . . . . . 8-2
- General SNMP Agent Configuration . . . . . 8-3

## 9 Packet Walk-Throughs

- Overview . . . . . 9-1
- Customer Packet Walk-Through . . . . . 9-1
- Management Packet Walk-Through . . . . . 9-3

## A Network Configuration Worksheets

- Overview . . . . . A-1
- Summarizing the Network Configuration . . . . . A-1
- Management Domain Configuration Worksheets . . . . . A-2
  - Assign an IP Address to the MCC Card . . . . . A-2
  - Assign an IP Address to the Backplane (s1b) . . . . . A-4
  - Assign IP Addresses to the DSL Cards . . . . . A-5
  - Create a Default Route . . . . . A-7
  - Reset the MCC Card . . . . . A-9
  - Configure the HotWire 5446 RTU Management Domain IP Addresses . . . . . A-10
  - Create a Static Route to the NMS . . . . . A-11
- Customer Domain Configuration Worksheets . . . . . A-14
  - Assign IP Addresses to the DSL Card LAN . . . . . A-15
  - Create Static Routes to End-User Systems . . . . . A-17
  - Create a Default Route or Source Route . . . . . A-18
  - Reset the DSL Card . . . . . A-20

## B IP Filtering Configuration Worksheets

- Overview . . . . . B-1
- Summarizing How to Define a Filter . . . . . B-1
- Filtering Configuration Worksheets . . . . . B-3
  - Defining the Filter and Rules . . . . . B-3
  - Binding the Filter . . . . . B-6

C SNMP Configuration Worksheets

- Overview . . . . . C-1
- Summarizing the General SNMP Agent Configuration . . . . . C-1
- SNMP Agent Configuration Worksheets . . . . . C-2
  - Defining a Community and Enabling Traps . . . . . C-2
  - Preventing Unauthorized Access . . . . . C-5

Glossary

Index

# About This Guide

## Document Purpose and Intended Audience

This guide describes the HotWire Digital Subscriber Line Access Multiplexer (DSLAM), its internetworking features, and how it works. It also provides information on what you need to know before planning your network. Use this guide to:

- Obtain a basic understanding of the HotWire DSLAM
- Understand how the DSLAM works within the network
- Understand the network model, management domain, and customer domain
- Understand how to allocate Internet Protocol (IP) addresses

This guide is intended for network planners, network administrators, and network maintainers. It is assumed that you have a basic understanding of internetworking protocols and their features. Specifically, you should have a basic familiarity with Simple Network Management Protocol (SNMP), Network Management Systems (NMSs), and the following internetworking concepts:

- TCP/IP applications
- IP and subnet addressing
- IP routing (also referred to as IP forwarding)

# Document Summary

| Section | Description |
|---|---|
| Chapter 1 | *Introduction to the HotWire DSLAM.* Provides an overview of the HotWire DSLAM and its components. It also briefly describes the network model and the domain types. |
| Chapter 2 | *Customer Domain Features.* Describes the features that are supported in the customer domain. |
| Chapter 3 | *Management Domain Features.* Describes the features that are supported in the management domain. |
| Chapter 4 | *Components of the Network Model.* Describes the components of the customer and management domains. These domains comprise the network model. |
| Chapter 5 | *IP Address Allocation.* Describes the IP address allocation schemes for the components that make up the network model. It also describes the naming convention used for the HotWire DSLAM system ports. |
| Chapter 6 | *IP Routing.* Provides information and examples of destination-based routing (static routes) and source-based routing. |
| Chapter 7 | *IP Filtering.* Describes IP filtering advantages and scenarios. |
| Chapter 8 | *SNMP Agent.* Describes the SNMP agent configuration (community configuration and trap configuration). |
| Chapter 9 | *Packet Walk-Throughs.* Provides examples of how data packets are routed through the customer network and the management network. |
| Appendix A | *Network Configuration Worksheets.* Provides worksheets to record your configuration settings. |
| Appendix B | *IP Filtering Configuration Worksheets.* Provides worksheets to help you define a filter for a specific interface on an MCC or DSL card. |
| Appendix C | *SNMP Configuration Worksheets.* Provides worksheets to help you set up community names and enable/disable the generation of alarms. |
| Glossary | Defines acronyms and terms used in this document. |
| Index | List key terms, acronyms, concepts, and sections in alphabetical order. |

# Product-Related Documents

| Document Number | Document Title |
|---|---|
| 5020-A2-GN10 | *HotWire POTS Splitter Central Office Installation Instructions* |
| 5030-A2-GN10 | *HotWire POTS Splitter Customer Premises Installation Instructions* |
| 5446-A2-GN10 | *HotWire 5446 Remote Termination Unit (RTU) Customer Premises Installation Instructions* |
| 7700-A2-GB23 | *DCE Manager for HP OpenView for Windows User's Guide* |
| 7800-A2-GB26 | *DCE Manager for HP OpenView User's Guide* |
| 8000-A2-GB20 | *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide* |
| 8000-A2-GN11 | *HotWire Management Communications Controller (MCC) Card Installation Instructions* |
| 8546-A2-GN10 | *HotWire 8546 Digital Subscriber Line (DSL) Card Installation Instructions* |
| 8600-A2-GN20 | *HotWire 8600 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide* |
| 8800-A2-GN21 | *HotWire 8800 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide* |

Contact your sales or service representative to order additional product documentation.

# Introduction to the HotWire DSLAM

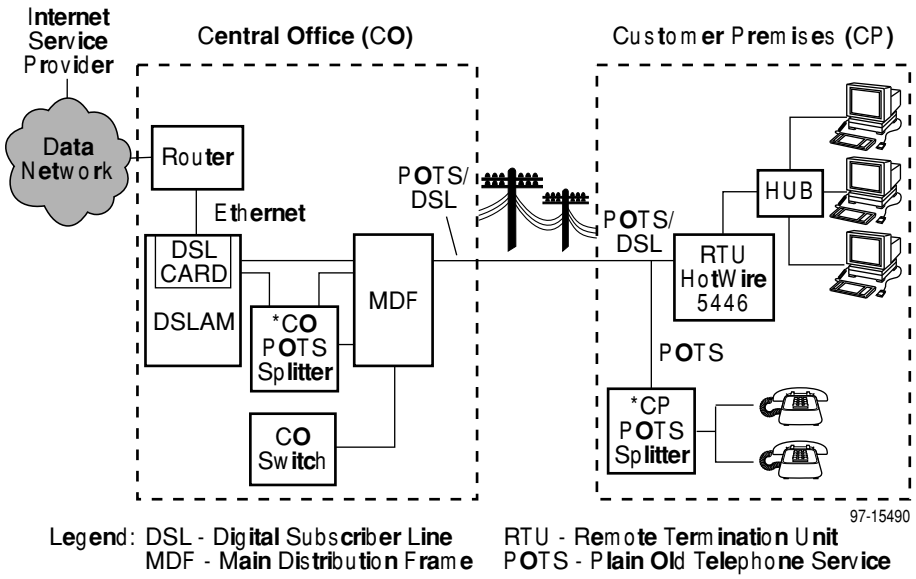
# 1

## What is the HotWire DSLAM?

The HotWire Digital Subscriber Line Access Multiplexer (DSLAM) is a DSL platform that interoperates with a HotWire 5446 Remote Termination Unit (RTU) to deliver applications at multimegabit speed in support of packet services over a Digital Subscriber Line (DSL) link.

High-speed service traffic types from the DSL links are groomed and then concentrated for efficient forwarding to backbone routers. By enabling very high speeds using DSL technology and then concentrating Internet Protocol (IP) traffic, greater performance is realized. Backbone service nodes can be placed deeper into the network, dramatically improving the economics of service provisioning while taking advantage of the substantial speed increases of DSL.

In addition, the HotWire DSLAM with the HotWire 5446 RTU can be multiplexed with Plain Old Telephone Service (POTS) over the same copper line providing simultaneous usage of POTS and digital application to separate locations. That is, the optional POTS Splitters (HotWire 5020 Central Office POTS Splitter and HotWire 5030 Customer Premises POTS Splitter) allow simultaneous voice and data connections over a standard telephone line.




# HotWire DSLAM Components

The HotWire DSLAM resides in a Central Office (CO) or wire center. It consists of the following components:

- HotWire DSLAM chassis
- MCC card
- DSL cards

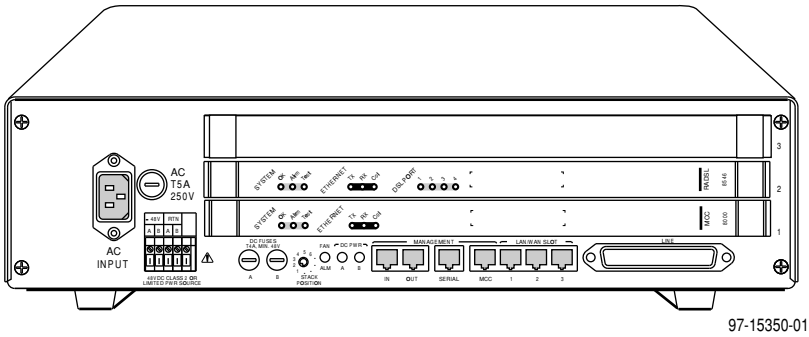
In addition, optional POTS Splitters can be installed at the CO. For information about a CO POTS Splitter, see the *HotWire POTS Splitter Central Office Installation Instructions*.

## HotWire DSLAM Chassis

There are two types of chassis:

- **HotWire 8600 DSLAM chassis**

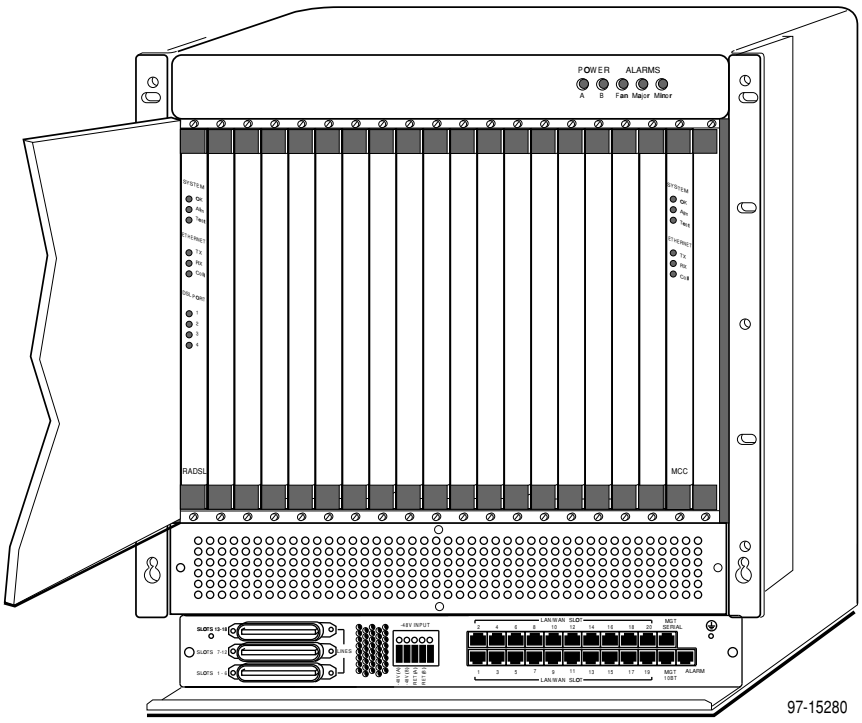
  The HotWire 8600 DSLAM is a low-cost alternative to the HotWire 8800 DSLAM. Each 8600 DSLAM chassis is an independent, stand-alone system. A stackable design provides for six systems to share management access through a single MCC card which, in turn, allows an additional slot for a DSL card in each of up to five systems. In a stacked configuration, the first or base chassis is equipped with an MCC card in Slot 1, leaving Slots 2 and 3 available for up to two DSL cards or a maximum of eight DSL ports. Each additional chassis houses up to three DSL cards. This stacking capability allows you to incrementally expand your DSL access service.




For more information about the HotWire 8600 DSLAM chassis, see the *HotWire 8600 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*.

- **HotWire 8800 DSLAM chassis**

  The HotWire 8800 DSLAM is a 20-slot chassis designed to house up to 18 DSL cards and one MCC card. (The remaining slot is reserved for future use.) The HotWire 8800 DSLAM chassis requires one MCC card and at least one DSL card.




For information about the HotWire 8800 DSLAM chassis, see the *HotWire 8800 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*.

## MCC Card

The MCC card is a single resource in the HotWire DSLAM that provides consolidated management access for the DSL cards and the HotWire 5446 RTU from any one of the following:

- SNMP management systems, such as Paradyne's DCE Manager
- Remote telnet sessions
- Local asynchronous terminal
- Remote asynchronous terminal connected to a modem

The MCC card connects to the NMS network via its 10BaseT interface. It performs alarm monitoring of the DSL cards, the HotWire DSLAM power and cooling systems, and interfaces to the CO alarm system. It also interfaces with external managers and servers (e.g., File Transfer Protocol servers) for system configuration and management.

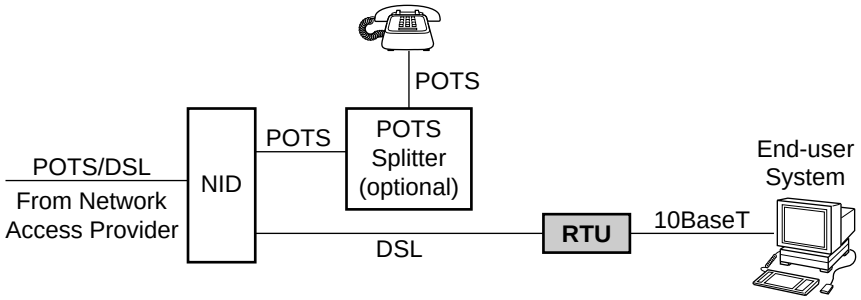
## DSL Cards

Each DSL card in the HotWire DSLAM chassis contains four DSL ports with on-board packet forwarding functionality. The outputs of the four DSL ports are combined onto one 10BaseT interface for connecting to the Internet or Intranet.

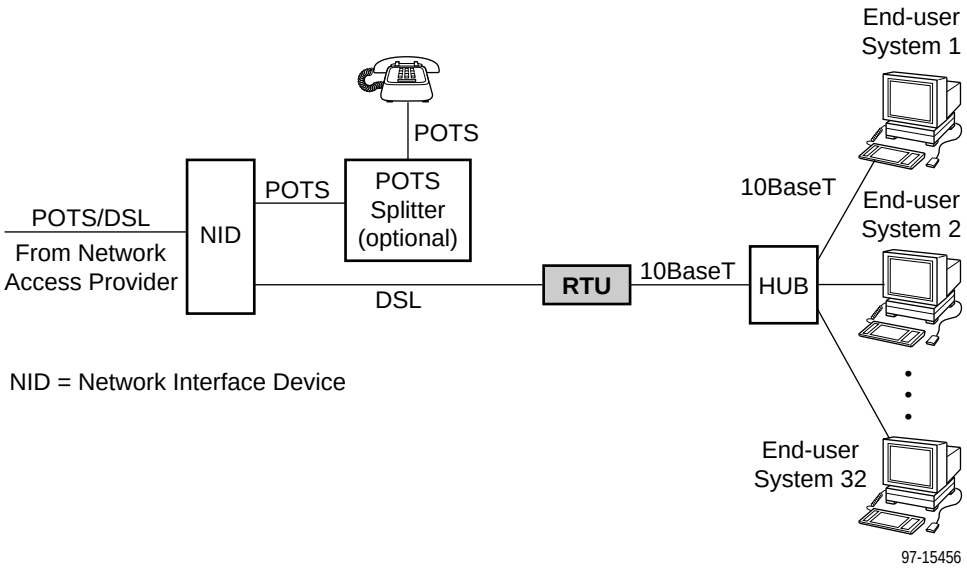
# What is the HotWire 5446 RTU?

The HotWire 5446 RTU resides at the customer premises and is composed of a DSL modem and an IP forwarder. The RTU connects to the local loop to provide high-speed connectivity to the HotWire DSLAM up to distances of 18,000 feet. You can connect the HotWire 5446 RTU directly to an end-user system or to multiple end-user systems via an Ethernet (10BaseT) hub. In addition, the RTU and telephone can function simultaneously over the same pair of copper wires at the customer premises when a POTS splitter is used at both ends of the local loop. The POTS splitter filters out the DSL signal and allows the POTS frequencies to pass through.

The following illustration shows the HotWire 5446 RTU with its 10BaseT interface connected directly to an end-user system (typically a PC or workstation with a Local Area Network (LAN) card).




The following illustration shows a HotWire 5446 RTU with its10BaseT hub connected to multiple end-user systems (each HotWire 5446 RTU can support up to four customer domains and up to 32 users). The other port of the HotWire 5446 RTU is a DSL interface connected to the HotWire DSLAM (over twisted-pair wiring). The POTS Splitter facilitates simultaneous voice and data transfer over a phone line.




For more information about the HotWire 5446 RTU, see the *HotWire 5446 Remote Termination Unit (RTU) Customer Premises Installation Instructions*. For information about the customer premises POTS splitter, see the *HotWire POTS Splitter Customer Premises Installation Instructions*.

# Overview of the HotWire DSLAM Network Model

The HotWire DSLAM and the HotWire 5446 RTU provide high-speed Internet or Intranet connectivity to a central site from customer premises.

**NOTE:**

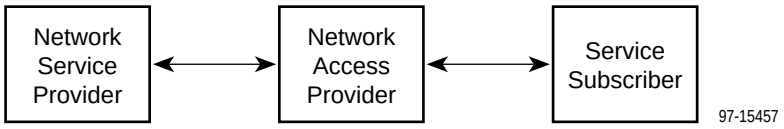
Data rates and distances vary depending on line speed and line conditions (i.e., the DSL cards measure performance during operation and can adjust the upstream or downstream rate to match changing loop characteristics due to temperature, humidity, or electrical interference). For a list of the supported DSL card data rates, see Appendix C, *Data Rates*, of the appropriate HotWire DSLAM Installation Guide.

The HotWire DSLAM network model can be implemented in a number of ways. For example:

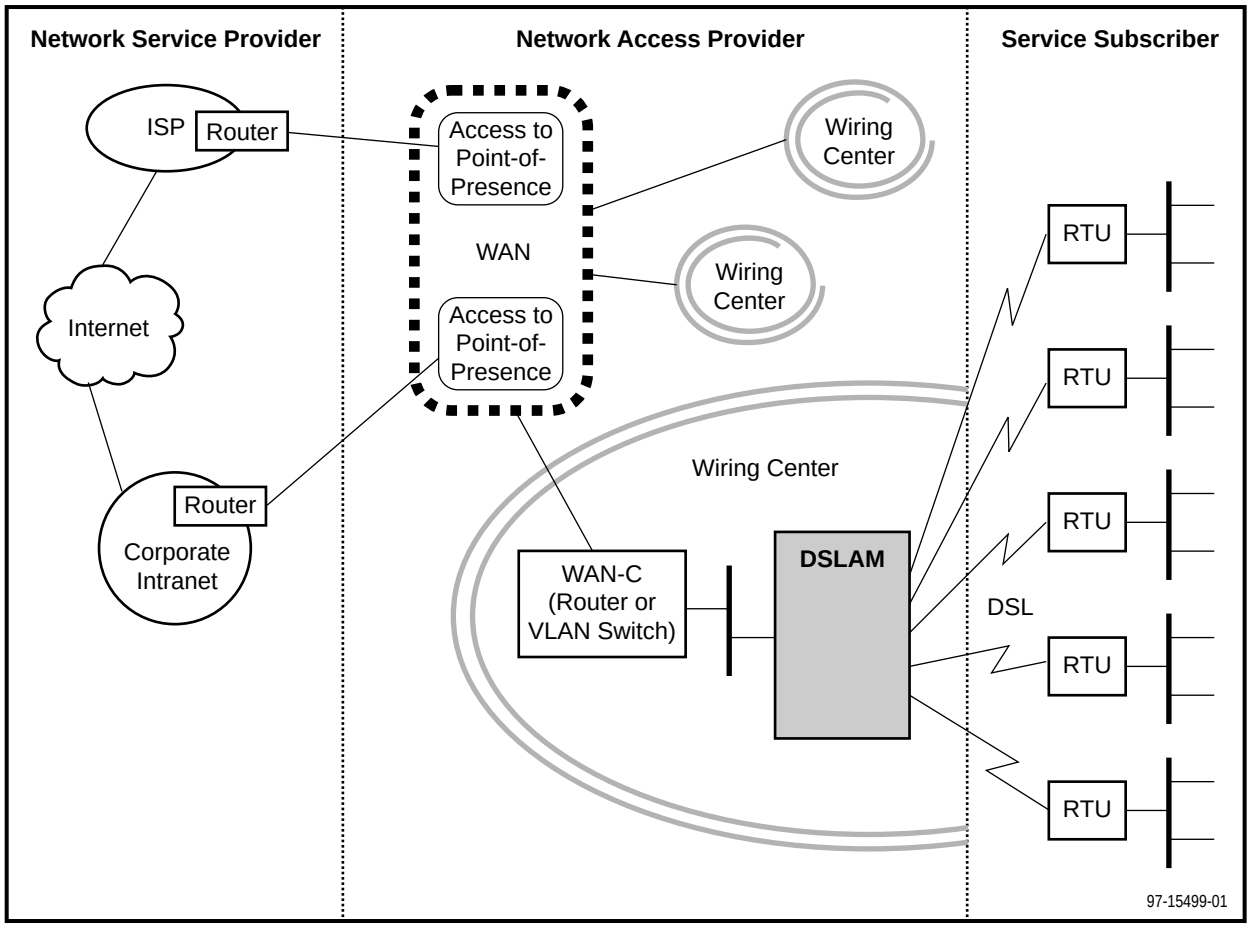
- A Small Office/Home Office (SOHO) implementation with one or more users connected to a LAN needing high-speed Internet connectivity to an Internet Service Provider (ISP).
- A SOHO implementation with one or more users connected to a LAN needing high-speed Intranet connectivity to the corporate LAN.
- A campus implementation needing internetworking between several sites, each with a LAN.

The network model for these examples can be partitioned into the following building blocks:

- **Network Service Provider**
- **Network Access Provider**
- **Service Subscriber**



The following illustration shows a detailed view of the network model:




- The **Service Subscriber** is the user (or set of users) that has contracted to receive networking services (e.g., Internet access, remote LAN access) from one or more Network Service Providers (NSPs). Service Subscribers may be:
  - — Residential users connected to public network services (e.g., the Internet)
  - — Work-at-home users connected to their corporate Intranet
  - — Commercial users at corporate locations (e.g., branch offices) connected to other corporate locations in their Intranet or connected to public network services

  RTUs must be installed at the customer premises to provide the Service Subscriber access to DSLs.
- The **Network Access Provider** (NAP) is typically the network provider (e.g., a Regional Bell Operating Company, an Alternate Local Exchange Carrier) that has access to the copper twisted pairs over which the DSLs operate. The NAP provides a transit network service permitting connection of service subscribers to NSPs.

Typically, the NAP network is organized into three components:

— **Wiring center**

The wiring center is usually a local serving office where the DSLs from the service subscribers are terminated on the HotWire DSLAM.

— **Wide Area Network (WAN)**

The WAN concentrates and switches data traffic from multiple wire centers to one or more Regional Centers.

— **Regional center**

The NSP's Point of Presence (POP) is located (i.e., access point to the NAP network for an NSP) at the regional center. The connection from the POP to the NSP network is typically across an access link that terminates on a router on the NSP premises. This router acts as a next-hop location to the NSP's network.

- The **Network Service Providers** (NSPs) can be either public data network providers (i.e., Internet Service Providers) or private data network providers (i.e., corporate Intranets) who provide network services based on the Internet Protocol (IP). In some cases, the NSP and the NAP can be a single network provider.

One or more HotWire DSLAMs are connected to a Wide Area Network Concentrator (WAN-C) via a LAN. The WAN-C concentrates data traffic from one or more DSLAMs onto facilities providing access to the WAN. The WAN-C can be either a router (a layer 3 networking device) or a VLAN switch (a layer 2 networking device).

- **If WAN-C is a router**, the WAN must be a routed IP network (i.e., a network comprised of IP routers interconnected via a point-to-point network, a frame relay switching network, or an Asynchronous Transfer Mode (ATM) switching network).

  In this case:

  — The router at the wiring center is required to support routing policies which permit packets arriving from the local DSLAMs to be routed based on the service subscriber source IP address to the appropriate router at the regional center containing the access to the POP for that NSP.

  — The routing tables in the DSLAM are configured such that the next-hop router points to the IP address of the wiring center router for all authorized subscriber IP source addresses. (See the discussion on source-based routing in Chapter 6, *IP Routing*.)

  If the DSLAM at that instance does not know the Media Access Control (MAC) address of the wire center router, it uses the Address Resolution Protocol (ARP) to obtain its MAC address from the wire center router prior to forwarding the packet. The router at the Regional Center must also route packets to the appropriate NSP based on the source IP address of the subscriber packets. In addition, the router at the regional center may need to participate in an exterior gateway protocol, such as the Border Gateway Protocol, to exchange routing information between the NSP and NAP routing networks.

— Packets flowing from the NSP network to the subscribers are routed within the NAP network based on the destination IP address (of the subscriber) as is most common for IP-routed networks.

- **If WAN-C is a VLAN switch**, the WAN must be a layer 2 switching network supporting a Virtual LAN overlay interconnected via a point-to-point network, a frame relay switching network, or an ATM switching network.

  In this case:

  — Each NSP would be a member of a different Virtual LAN.

  — The VLAN switch at the wiring center would support either port-based VLAN switching (i.e., switching all MAC frames received on a specific port to a specific NSP VLAN on the WAN) or port-based VLAN switching with MAC-based attributes (i.e., switching frames received on a specific port to a specific NSP VLAN on the WAN based on the destination MAC address) for packets sent from the DSLAMs.

  — The router at the NSP premises would either be front ended by a VLAN switch or have an integrated VLAN card that supports protocols consistent with the wire center VLAN switch (e.g., ATM Forum LAN Emulation Protocol).

  — The routing tables in the DSLAM are configured such that the next-hop router points to the IP address of the NSP premises router for all authorized subscriber IP source addresses associated with the address domain of that NSP. (See the discussion on source-based routing in Chapter 6, *IP Routing*.)

  — A different next-hop router is specified for each NSP address domain in contrast to the routed network case where a single next-hop router was specified for all NSP domains. If the DSLAM at that instance does not know the MAC address of the NSP premises router, it uses ARP to obtain its MAC address from the NSP premises router (i.e., the wire center VLAN switch forwards an ARP request over the WAN to the NSP router) prior to forwarding the packet.

  — Packets flowing from the NSP network to the subscribers are routed to the subscriber based on the destination IP address (of the subscriber) as is most common for IP-routed networks. In this case, the LAN on which the DSLAM resides appears to be part of a local subnet connected directly to the NSP premises router. If the NSP router at that instance does not know the MAC address of the subscriber, it uses ARP to obtain the MAC address from the DSLAM that acts as a proxy for the subscriber. (See the discussion on proxy ARP in Chapter 2, *Customer Domain Features*.)

# Understanding the Domain Types

Functionally, the HotWire DSLAM network model can be divided into:

- Features supporting customers

  Features integral to supporting customers are the DSL cards and HotWire 5446 RTUs.

- Features supporting overall system management

  The central point of access for overall system management is the MCC card. However, the features integral to supporting overall system management are also distributed throughout the HotWire DSLAM and the HotWire 5446 RTUs.

To monitor and control the operation of the overall system, the IP addresses of the HotWire DSLAM and the HotWire 5446 RTU must be allocated in such a way that they are partitioned into two distinct domains.

- **Management domain**

  The management domain resides in a mutually-exclusive domain from that of the customer domain. The NAP provisions IP addresses for the management domain.

  For more information about the management domain, its features and components, see Chapters 3 and 4.

- **Customer domain(s)**

  The customer domain (also known as the ISP domain) resides in a mutually-exclusive domain from that of the management domain. (There should be one customer domain for each NSP served by the HotWire DSLAM.) A customer domain encompasses IP addresses in all ISP domains to which the end-user systems (ES) subscribe.

  For more information about the customer domain, its features and components, see Chapters 2 and 4.

For more information about assigning IP addresses, see Chapter 5.

# Customer Domain Features

# 2

## Overview

This chapter describes the following features that are supported in the customer domain:

- Data Rates
- Protocols
- Address Resolution Protocol (ARP) with Proxy ARP
- Filtering

## Data Rates

The HotWire DSL card employs Rate Adaptive Digital Subscriber Line (RADSL) devices based on Carrierless Amplitude & Phase (CAP) technology. The RADSL speed is asymmetric. This means that the downstream rate (from the DSLAM to the RTU) is faster than the upstream rate (from the RTU to the DSLAM).

You can manually set the speed (providing the line you are using can support the specified speed) or set the speed to auto-select. The HotWire DSLAM determines the line speed during the initial handshaking session between the DSLAM and the RTU based on the loop length, the amount of noise on the loop, and the user-configurable upper and lower speed limits.

The following are the maximum upstream and downstream data rates with standard #24 AWG wiring, and 24 ISDN disturbers in the same 25-pair binder group:

- Maximum upstream data rate: 1088 kbps (remote access from the customer premises to the CO up to a distance of 13,400 feet)
- Maximum downstream data rate: 2560 kbps (remote access from the customer premises to the CO up to a distance of 15,600 feet)

The following are the maximum upstream and downstream data rates with standard #26 AWG wiring, and 24 ISDN disturbers in the same 25-pair binder group:

- Maximum upstream data rate: 1088 kbps (remote access from the customer premises to the CO up to a distance of 8,300 feet)
- Maximum downstream data rate: 2560 kbps (remote access from the customer premises to the CO up to a distance of 12,300 feet)

For a complete listing of the DSL card data rates, see Appendix C, *Data Rates*, of the appropriate HotWire DSLAM Installation Guide. For information on how to set the line speed, see Chapter 6, *DSL Card Configuration*, of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide.*

# Protocols

The HotWire DSLAM and HotWire 5446 RTU forward IP packets between the end-user system and the Network Service Provider using the following protocols:

- **Point-to-Point Protocol/High-level Data Link Control (PPP/HDLC)**

  Packets transmitted over DSL ports are encapsulated in PPP/HDLC.

- **MAC**

  Packets transmitted over LAN ports are encapsulated in IEEE 802.3 MAC.

- **IP**

  IP packets arriving over the DSL interface are IP forwarded to the LAN interface. IP packets arriving over the LAN interface are IP forwarded to the appropriate DSL interface.

  **NOTE:**

  *Directed broadcasts* (also referred to as *subnet broadcasts* — all 1s (ones) in the host field) are forwarded upstream, but are not forwarded downstream.

  Also, multicasting is not supported.

- **Internet Control Management Protocol (ICMP)**

  In general, ICMP is supported. It should be noted, however, that the options field is not reflected back if the HotWire DSLAM is the destination address (i.e., the options field is stripped from the packet when the HotWire DSLAM receives the data and then returns the packet without the options field). The HotWire DSLAM does, however, pass the packet with the options field to the next-hop if the DSLAM is not specified as the destination address.

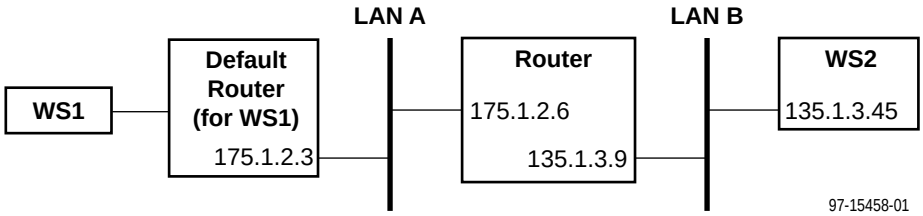
# Proxy ARP (Theory of Operation)

An Address Resolution Protocol (ARP) request is used to dynamically bind an IP address to a MAC address. Proxy ARP is a technique by which a router answers ARP requests intended for another machine by supplying its own MAC address (also referred to as the physical address). By answering for another device, the router accepts responsibility for forwarding packets to that device.

ARP is supported by the MCC and DSL cards, and the HotWire 5446 RTU. Proxy ARP allows the end users to appear to be directly connected to the router or VLAN switch providing access to the ISP network. This is an advantage because routers connected to a device running proxy ARP require less configuration. The following scenarios show why this is an advantage.

## Scenario 1: Without Proxy ARP

In this scenario, a router does not have proxy ARP software and the networks of the default router for workstation 1 (175.1.2.3) and workstation 2 (135.1.3.45) are different.



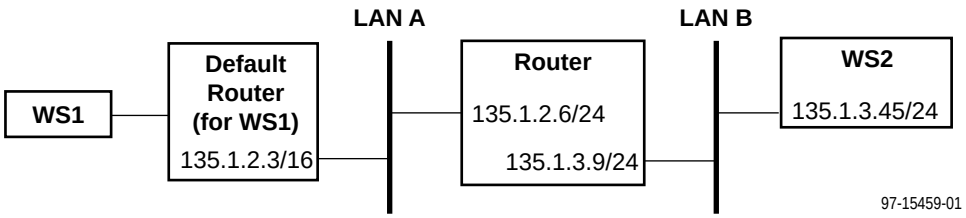

Workstation 1 (WS1) needs to send a packet to workstation 2 (WS2). For the packet to arrive successfully at WS2:

- Configure a static route on the default router for WS2 (the next hop being the router and the destination being WS2).
- WS1 sends a packet to the default router.
- The default router consults its routing table to determine the next hop address (i.e., router IP address) for WS2 because WS2 is on another network (135.1.0.0).

Now that it knows the next hop address to the router, the default router then ARPs for the router. The router receives the ARP request for its IP address and does an ARP reply with its MAC address (also known as the physical address). After the default router receives the ARP reply, it sends the packet to the router which, in turn, forwards it to WS2.

## Scenario 2: With Proxy ARP

In this scenario, a router is running the proxy ARP software, and WS2 and the default router for WS1 are on the same network (135.1.0.0).




WS1 again needs to send a packet to WS2. This time, however, the router is running proxy ARP and knows that WS2 lies on LAN B on the same logical subnetwork as the default router (135.1.0.0). The router uses proxy ARP to maintain the illusion that only one physical network exists. The router keeps the location of WS2 hidden from the default router, allowing the default router to communicate as if directly connected to WS2.

**NOTE:**

The default router does not need a static route entry for the WS2 route because the two LANs appear to be one.

Therefore, when WS1 needs to send a packet to WS2, this is the sequence of events:

- WS1 sends a packet to its default router.
- The default router invokes ARP to map the WS2's IP address into a MAC address.
- The router running proxy ARP software receives the broadcast ARP request from the default router, knows that WS2 is on LAN B, and responds to the default router's ARP request with its own MAC address.
- The default router receives the ARP reply, then sends the packet to the MAC address of the router.
- The router then forwards the packet destined for WS2 on LAN B.

The proxy ARP capability is card or system dependent and detailed examples for the MCC card, DSL card, and HotWire 5446 RTU are given in Chapter 4.

# Filtering

By default, filtering is disabled on the HotWire DSLAM system, but you can enable filtering to selectively filter source or destination packets being routed through the MCC or DSL cards. Filtering provides security advantages on LANs by restricting traffic on the network and hosts based on the IP source/destination address.

**NOTE:**

Each time you create a static route for an end-user system behind an RTU, you should also create a corresponding filter.

For more information about filtering, see Chapter 7, *IP Filtering*.

# Management Domain Features

# 3

## Overview

This chapter describes the following features that are supported in the management domain:

- Network Management Systems (NMSs)
- Applications for Diagnostics

## Network Management Systems — SNMP and DCE Manager

You may want to use an SNMP NMS, such as Paradyne's DCE Manager for HP OpenView (UNIX) or DCE Manager for HP OpenView for Windows (MS Windows), to simplify the operation and management of very large networks. DCE Manager allows you to monitor and manage your network from a central point The HotWire DSLAM and HotWire 5446 RTU provide features for DCE Manager to do just that by using SNMP and HP OpenView.

The following lists some of the features of DCE Manager:

- Graphical User Interface (GUI) showing physical representation of the HotWire DSLAM
- Multiple integrated functions to provide on-demand health and status information
- Color-coded graphic representations to provide instant visual status
- Loopback and pattern tests via telnet to help isolate problems quickly
- Integrated management optimizes network performance and availability
- Direct telnet support

These SNMP capabilities provided by Paradyne's DCE Manager provide access to MIB II, Entity MIB, and private-enterprise MIB extensions to facilitate:

- Monitoring and uploading/downloading configuration information from the HotWire DSLAM, and
- Monitoring and uploading/downloading information to the MCC card, DSL cards, and HotWire 5446 RTU.

The DSLAM uses a processor card called the Management Communications Controller (MCC) card in conjunction with DCE Manager. The MCC card provides the single point of contact to the DSL card and HotWire 5446 RTUs. It gathers operational status for each of the HotWire DSL cards in the DSLAM and reports events and alarms to the DCE Manager. For more information, see the *DCE Manager for HP OpenView for Windows User's Guide* or the *DCE Manager for HP OpenView User's Guide*.

# Applications for Management

The HotWire DSLAM user interface provides the following management applications:

- Ping
- tFTP client
- Telnet

## Ping

The ping program, which is an IP-based application used to test reachability of destinations by sending them an ICMP echo request and waiting for a reply, is supported from both the DSL and MCC cards. As a diagnostic tool, the ping program from the MCC card can be used to verify reachability in the management domain to the DSL card, the HotWire 5446 RTU, and to the DCE manager. Similarly, invoking the ping program from the DSL card can be used to verify reachability downstream to the HotWire 5446 RTU and the ES, and to verify reachability upstream to the ISP.

**NOTE:**

Record route and other ICMP options facilitating trace route are also supported. However, the options field is not reflected back if the HotWire DSLAM is the destination address (i.e., the options field is stripped from the packet when the HotWire DSLAM returns the packet). The HotWire DSLAM does, however, pass the packet with the options field to the next hop if the DSLAM is not specified as the destination address.

For more information, see Chapter 8, *Diagnostics and Troubleshooting*, of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

## tFTP Client

The MCC card and DSL card each provide client trivial File Transfer Protocol (tFTP) applications that work with the firmware download and configuration upload or download features. tFTP sessions are established between the MCC card or the DSL card to a tFTP server accessible through the LAN interfaces during these data transfers.

A recommended use for configuration transfers is to upload a DSL card configuration to save (archive) the configuration set. Then, if necessary, you can recover the configuration by downloading (restoring) the saved configuration.

For more information, see Chapter 5, *MCC Card Configuration*, Chapter 6, *DSL Card Configuration*, and Appendix D, *Download and Apply Code*, of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

## Telnet

The HotWire DSLAM system provides support for telnet, which is a simple remote terminal protocol that is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. With telnet, a network administrator can establish a virtual access connection to the HotWire DSLAM from a remote client to configure or monitor the HotWire DSLAM. You will see the same local user interface during a telnet session to the HotWire DSLAM.

A telnet connection from the HotWire DSLAM to another HotWire DSLAM or remote server is also supported. This feature is supported from the Ethernet (10BaseT) interface on the MCC card or DSL card.

For more information, see Chapter 8, *Diagnostics and Troubleshooting*, of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

# Components of the Network Model

# 4

## Overview

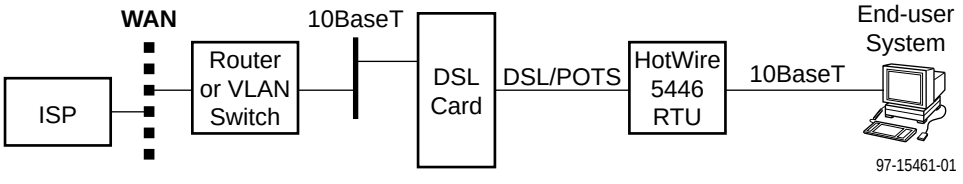
The customer and management domains logically comprise the network model. This chapter describes the components that comprise these domains.

## Customer Domain Components

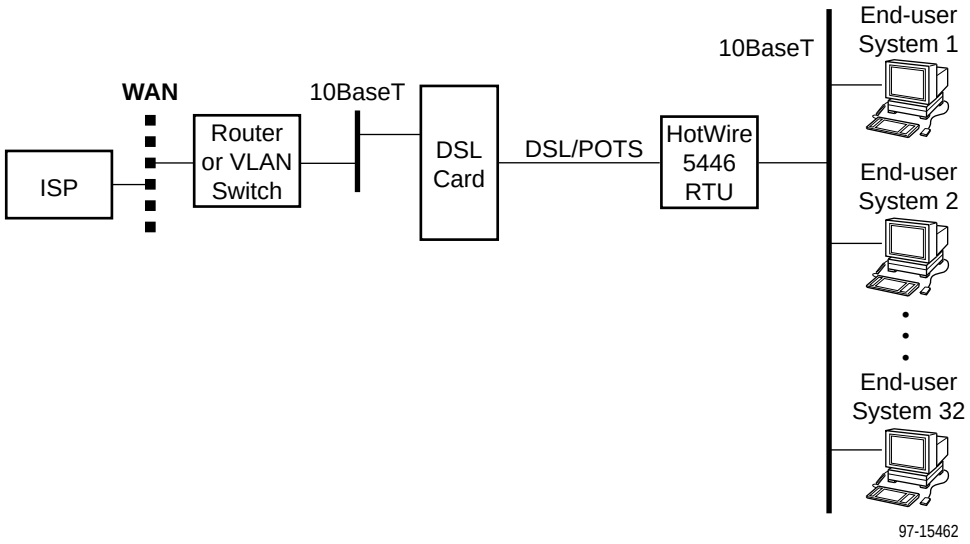
The primary purpose of the customer domain network is to provide IP routing of customer data between the Internet Service Provider (ISP) and the end-user system (ES).

The basic customer domain configuration consists of the following components:

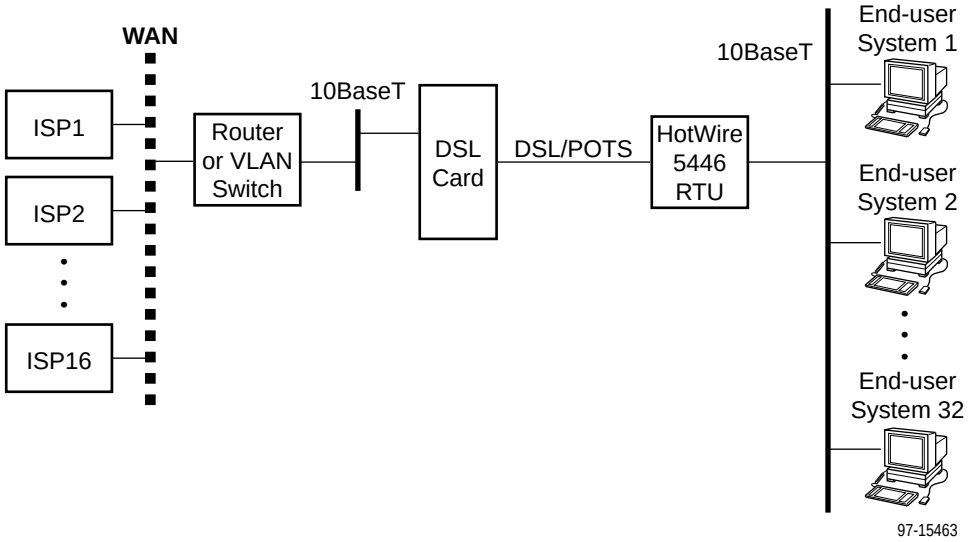
- An end user (PC or workstation) or multiple users on a subnet connected to the HotWire 5446 RTU, which in turn, is connected to one of the DSL card ports of the HotWire DSLAM
- The 10BaseT port of the HotWire DSLAM DSL card connected to a router that may also reside in the Central Office (CO) or wire center
- The router is then connected to the ISP typically over a Wide Area Network (WAN)
- The ISP may also be directly connected to the same LAN as the DSL card



The following illustration shows another internetworking configuration. This configuration has multiple end users connected to the HotWire 5446 RTU using a hub. The number of supported end-user systems depends on what route type is used (host or structured subnetting). For more information, see Chapter 5, *IP Address Allocation*.




When multiple end users are connected, they may opt to access different ISPs, as illustrated below. When all 18 DSL cards are used, the HotWire DSLAM can support simultaneous access up to 288 different ISPs or private intranets by the end users (16 ISPs or private intranets per DSL card).



When your HotWire DSLAM system is maximally configured, more users can be supported. With a maximally-configured HotWire DSLAM system (i.e., a HotWire DSLAM with 18 DSL cards with each DSL card having its four ports connected to a HotWire 5446 RTU for a total of 72 modem ports, and each modem can connect via a hub to 32 active end systems), a total of 2304 users can be supported. Additionally, by setting up structured subnets behind each HotWire 5446 RTU, hundreds of active end systems can be supported by each RTU instead of 32. Careful network traffic analysis must be performed to determine if very large networks will have acceptable response times. For information on how to set up structured subnets, see Chapter 5, *IP Address Allocation*.

**NOTE:**

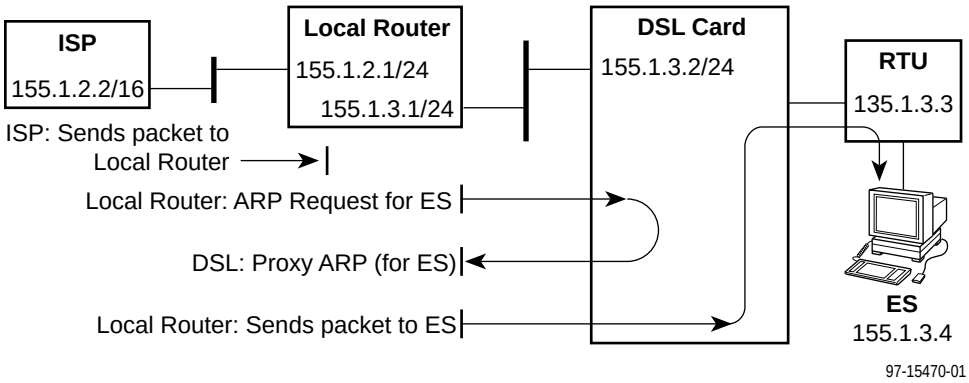
Usually a user is active only in one domain at a time. However, if the user's system can be multihomed, it may be possible to be active in more than one domain at a time. A **multihomed** system is a system with connections to two or more logical networks, which may be assigned to one or more physical networks.

## Proxy ARP

Proxy ARP is supported by the DSL cards and the HotWire 5446 RTU. It allows the end users to appear to be directly connected to the router providing access to the ISP network. This is an advantage because routers connected to a device running proxy ARP require less configuration. The following scenarios show why this is an advantage.

### DSL Card Proxy ARP

When an ARP request is sent by an ISP connected to the DSL card 10BaseT interface for a downstream ES (one on the same IP network), the DSL card will proxy ARP for the ES. The following figure shows the packet flow when the ISP wants to send a packet to the ES.



In this illustration:

- The local router does an ARP request for the ES.
- The DSL card receives the broadcast ARP request. The DSL card does an ARP reply for the ES by replying with its own MAC address. Addresses for which the DSL card will proxy ARP must be configured as part of static route configuration. See the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide* for more information.
- When the local router receives the ARP reply, it sends the packet to the DSL card, and the DSL card forwards it to the ES.

**NOTE:**

In certain network configurations, the use of proxy ARP on the DSL cards will cause HP OpenView to log a major event. This will happen since HP OpenView received the same IP address from two different MAC addresses.

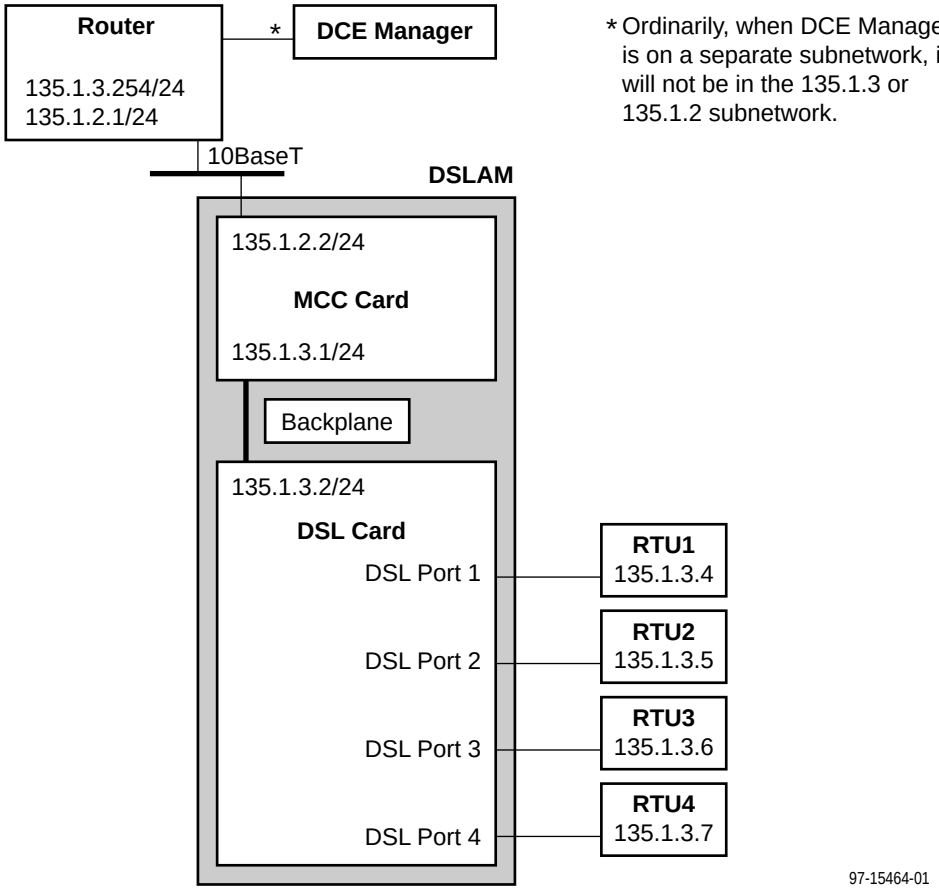
By default, the HP OpenView system logs and displays all events. However, you may elect to filter specific unwanted events. Instructions on how to filter out these events are dependent on the release of HP OpenView/Netview that you are running. For detailed instructions, see the appropriate HP OpenView user documentation.

### HotWire 5446 RTU Proxy ARP

The HotWire 5446 RTU utilizes proxy ARP to enable connectivity between end systems that are attached to separate RTUs, but reside on the same subnetwork. The HotWire 5446 RTU will proxy ARP for the end-user system that is physically connected to another HotWire 5446 RTU where the destination end-user system is logically connected to the same subnetwork as the sender end-user system.

# Management Domain Components

The following illustration shows the components of the network management domain. Note that the router between the MCC card's 10BaseT interface and the DCE Manager is optional. The MCC card, as previously noted, provides consolidated management for the DSL cards and HotWire 5446 RTUs from SNMP workstations or its VT100 interface.




To facilitate management of the DSL cards and HotWire 5446 RTUs through the MCC card:

- Assign IP addresses to the internal backplane interfaces of each DSL card and each HotWire 5446 RTU interface in the same subnet as the MCC card's backplane (as shown in the previous illustration).

  These IP addresses are stored in the Entity MIB on the MCC card where they can be accessed by the DCE Manager.

- Provide IP addresses on the router's interface attached to the MCC card for both subnetworks, so that the router appears to be directly connected to the MCC card's Ethernet interface as well as the HotWire DSLAM system backplane.

In other words, the router's interface to the MCC must be multihomed. This is necessary to support proxy ARP.

## Discovering Devices on the Network (Discovery)

In the illustration on page 4-5, the IP addresses assigned for the router's interface to the MCC card are 135.1.2.1 and 135.1.3.254. The second IP address is on the same subnetwork as the internal addresses of the DSL cards and the HotWire 5446 RTUs. The MCC card will not forward broadcasts on the management network (135.1.2.x) across the HotWire DSLAM system backplane because it is a separate subnetwork, as the DSL cards do not need to be *discovered* by the management system.

**How does the NMS learn the address of a device beyond the MCC card?**

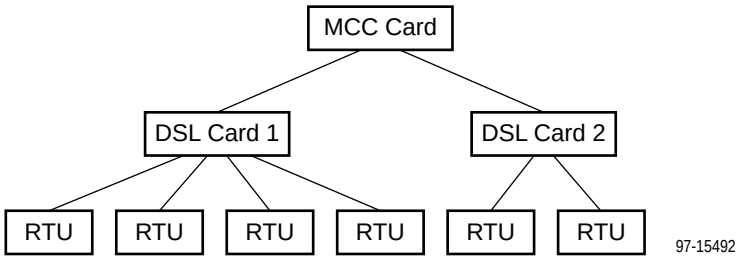
- DCE Manager gets the IP address of a DSL card from the Entity MIB on the MCC card.

  After the DCE Manager has learned the IP address of a DSL card through the Entity MIB, it addresses management traffic directly to that card.

- DCE Manager gets IP address of the RTU from the Entity MIB on the DSL card.

  After the DCE Manager has learned the IP address of the RTU through the Entity MIB, it addresses management traffic directly to that RTU.

When the HotWire DSLAM and HotWire 5446 systems networks are configured as described above, the DCE Manager provides a view of the entire network from information contained in the MCC card's entity MIB.




### NOTE:

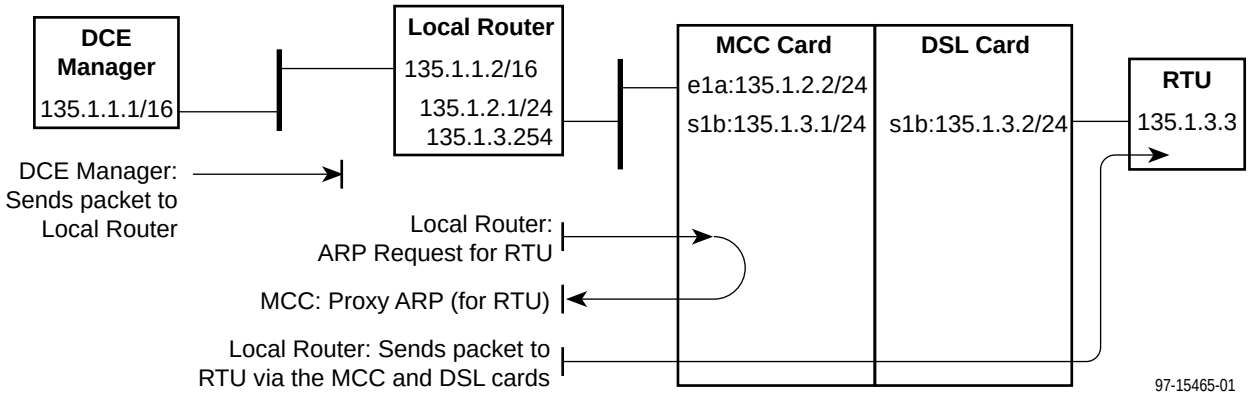
It is not recommended that the DCE Manager access a DSL card via its Ethernet port because the Entity MIB on the DSL card does not reflect a view of the entire HotWire DSLAM system. It reflects only the view of the DSL card *discovered*. Also, in a fully configured DSLAM, 18 additional devices will be discovered and appear on your network map.

If you want to manage DSL devices across the ISP network, use telnet. For more information on telnet see Chapter 8, *Diagnostics and Troubleshooting*, of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

## MCC Card Proxy ARP

Proxy ARP is also supported by the MCC card. In a HotWire DSLAM network configuration, when an ARP request is sent by a device (such as a router) to the MCC card's 10BaseT interface to resolve either the DSL card or HotWire 5446 MAC address, the MCC card will proxy ARP for those devices so long as their IP addresses are on the same network (135.1.3.x). The MCC card responds to these ARP requests with its own MAC address (proxy ARP). Incoming packets are then forwarded to that appropriate DSL card across the HotWire DSLAM system backplane.

The following illustration shows the packet flow when the DCE Manager wants to send a packet to the HotWire 5446 RTU.




In this illustration:

- The local router does an ARP request to resolve the HotWire 5446 MAC address.
- The MCC card is in the same network (135.1.3.1). It sees the ARP request. The MCC card knows that the HotWire 5446 is downstream, because it contains a route to it (generally a host route). The MCC card does an ARP reply for the HotWire 5446 by responding with its own MAC address.
- When the local router receives the ARP reply, it forwards the packet to the MCC card.
- After receiving the packet, the MCC card forwards it to the DSL card which forwards it to the HotWire 5446 RTU.

# IP Address Allocation

# 5

## Overview

IP addresses are assigned throughout the network model for components comprising both the customer and management domains. This chapter describes the IP address allocation schemes for the components that make up the HotWire DSLAM network model. It also describes the naming convention used for the HotWire DSLAM system interfaces.

## Port Naming Convention

The following is the naming convention used for the HotWire DSLAM interfaces:

**NOTE:**

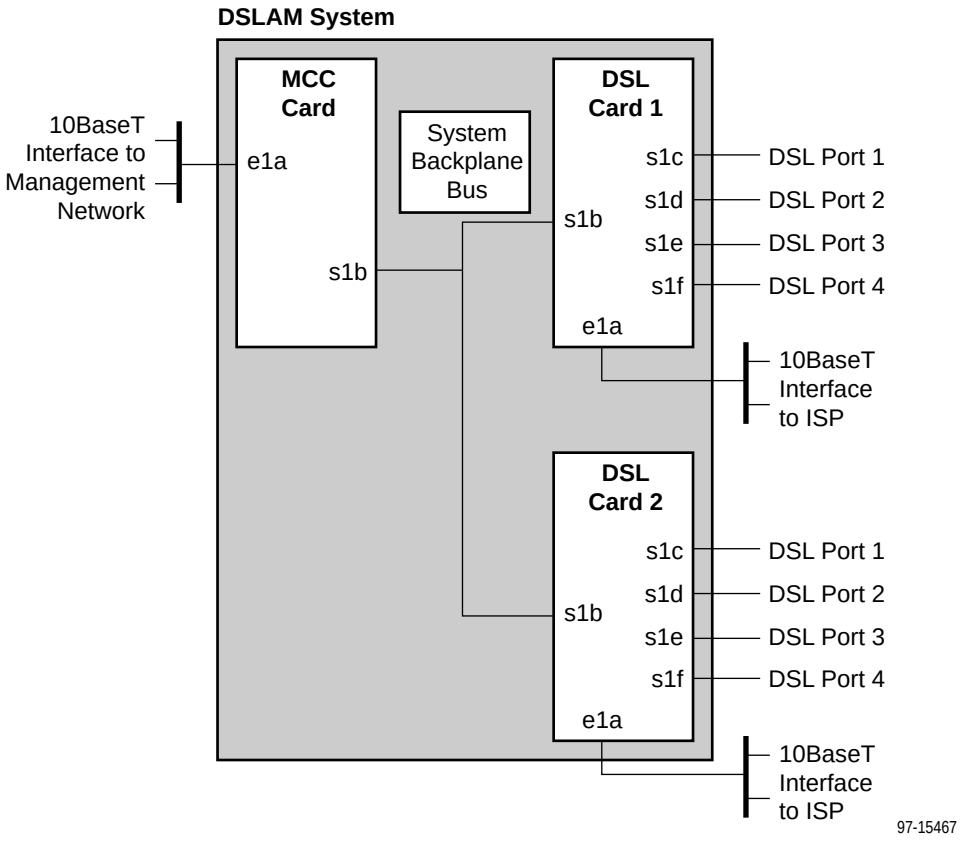
Interfaces are sometimes referred to as ports. The term *ports*, however, usually is reserved for referring to the physical layer attributes of an interface.

- **e1a** — Interface name of the DSLAM system 10BaseT interface on the MCC and DSL cards.
- **s1b** — Interface name of the card's interface to the DSLAM system backplane bus.
- **s1c**, **s1d**, **s1e**, and **s1f** — Interface names of the four DSL ports on a DSL card.

**NOTE:**

These names are used throughout the remainder of this guide to reference the HotWire DSLAM interfaces. These are also the names used in the HotWire DSLAM software when configuring the HotWire DSLAM system.

The following illustrates the logical interface naming convention.




# Assigning IP Addresses

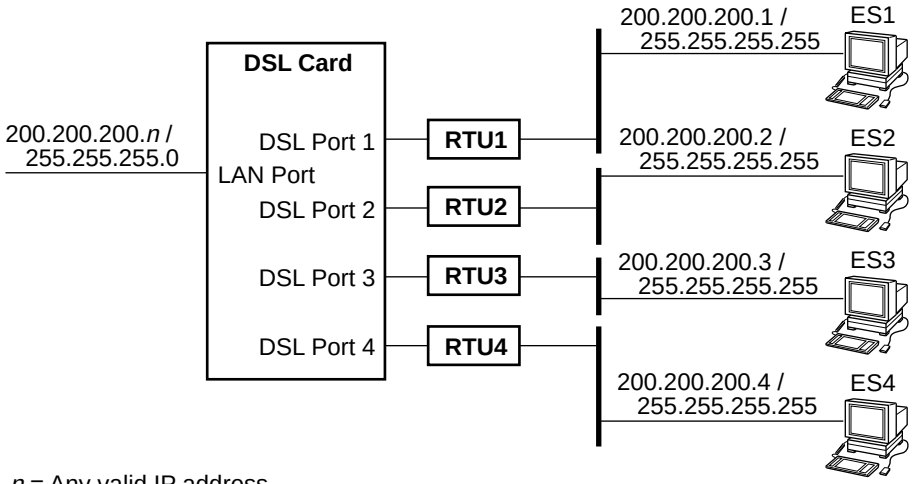
In the HotWire DSLAM network model, there are two distinct domains: a management domain and a customer domain.

Within the management domain, there are two subnets as described in the *Management Domain Components* section in Chapter 4, *Components of the Network Model*. Within the customer domain, one of two IP address allocation schemes can be followed: host addressing or structured subnet addressing. The following sections describe these schemes.

## Host Addressing

Host addresses within the customer domain are assigned to end-user systems. Because they are host addresses, they have a subnet mask of 255.255.255.255 and can be geographically dispersed. This conserves address space, but may not scale well to large numbers of end-users. Manual configuration is required for every host address and routing performance may be decreased.

The following illustration is an example of host addressing.



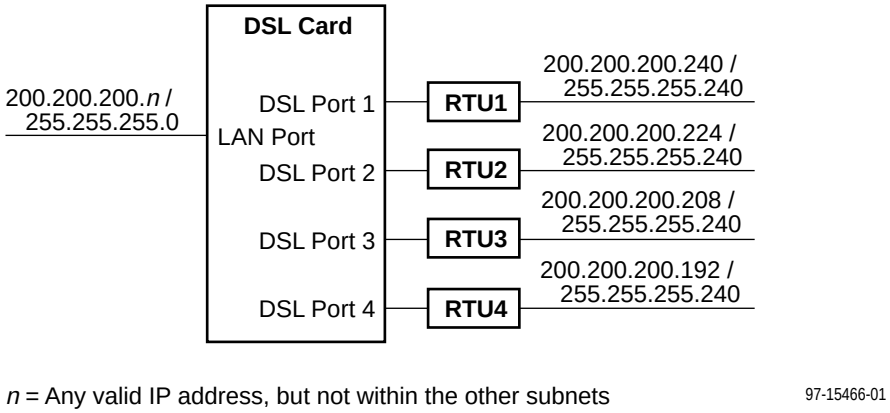

## Structured Subnet Addressing

As an alternative to using host routes for end-user systems, structured subnetting can be used. It scales better and performs better, but it does not allow geographically-dispersed subnets.

Structured subnet addressing uses the following method:

- Within the customer domain, the ISP would provision a subnet of its domain to a DSL card and all devices behind it.
- The ISP would further subdivide that subnet into four additional subnets (one behind each DSL port).

The following illustration is an example of structured subnet addressing.



To understand why this subnetting scheme works, you may want to consider the IP addresses and subnet masks in hexadecimal:

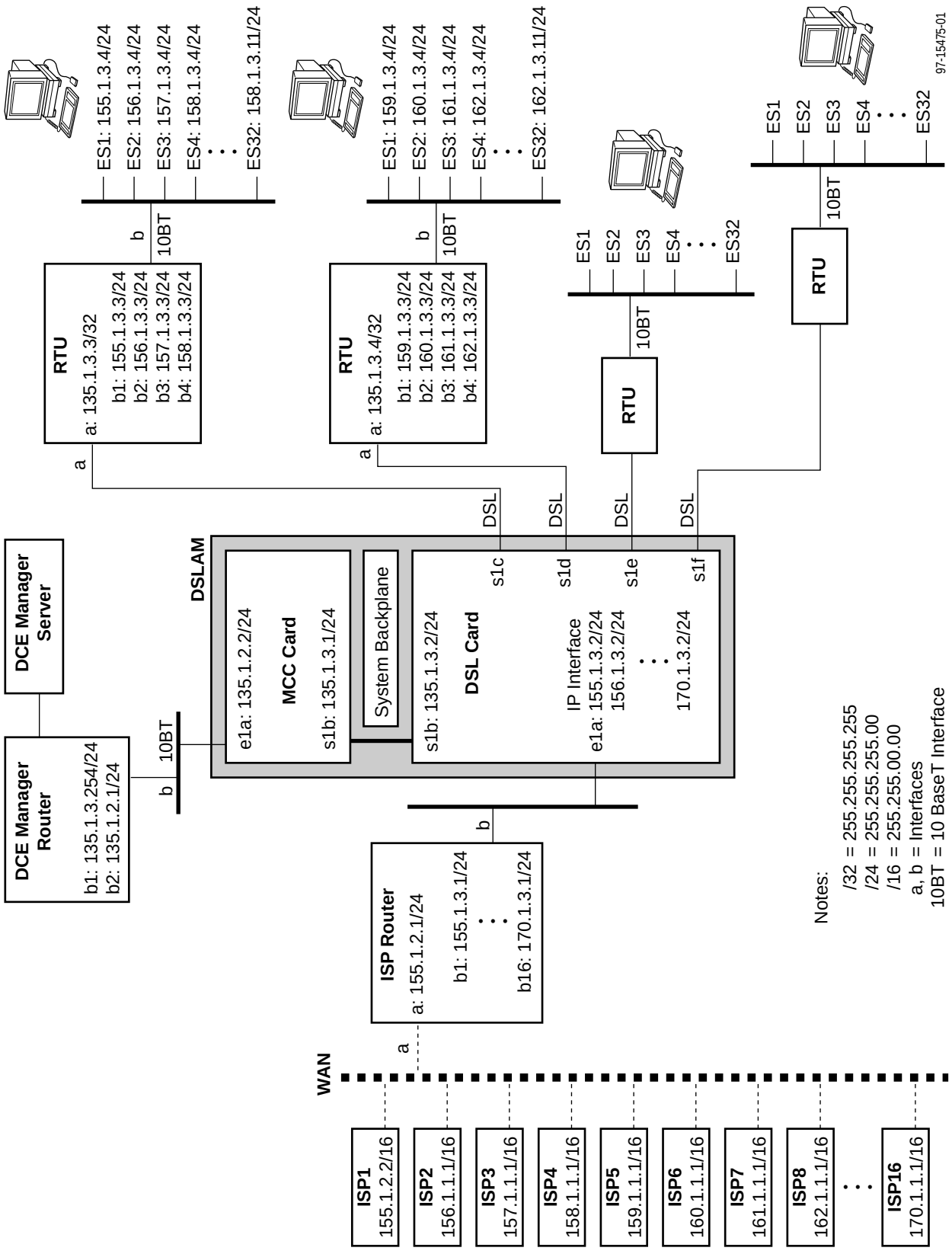
| Dotted Decimal | Dotted Hexadecimal |
|---|---|
| 200.200.200.00 / 255.255.255.0 | C8.C8.C8.00 / FF.FF.FF.00 |
| 200.200.200.240 / 255.255.255.240 | C8.C8.C8.F0 / FF.FF.FF.F0 |
| 200.200.200.224 / 255.255.255.240 | C8.C8.C8.E0 / FF.FF.FF.F0 |
| 200.200.200.208 / 255.255.255.240 | C8.C8.C8.D0 / FF.FF.FF.F0 |
| 200.200.200.192 / 255.255.255.240 | C8.C8.C8.C0 / FF.FF.FF.F0 |

In this illustration:

- Each of the four DSL ports is on a different subnetwork and the subnet mask for the four ports is 255.255.255.240.
- The LAN port (10BaseT port) IP address is 200.200.200.*n* (where *n* can be any valid IP address, but cannot be an IP address within the other subnets) and its subnet mask is 255.255.255.0.

The illustration on page 5-5 shows an example of overall structured subnetting. In this illustration, 16 ISPs are connected to one DSL card. The ISP router is multihomed to support all 16 ISPs. Also, each RTU has 32 end-user systems (ES).

In summary, if 32 end-user systems are connected to the DSL card's port 1 and all are using host addressing, then 32 host routes must be configured on the RTU. If they are using structured subnet addressing, then only one route is configured on the RTU.


ES1: 155.1.3.4/24
ES2: 156.1.3.4/24
ES3: 157.1.3.4/24
ES4: 158.1.3.4/24
ES32: 158.1.3.11/24
ES1: 159.1.3.4/24
ES2: 160.1.3.4/24
ES3: 161.1.3.4/24
ES4: 162.1.3.4/24
ES32: 162.1.3.11/24
ES1
ES2
ES3
ES4
ES32
97-15475-01
RTU
a: 135.1.3.3/32
b1: 155.1.3.3/24
b2: 156.1.3.3/24
b3: 157.1.3.3/24
b4: 158.1.3.3/24
RTU
a: 135.1.3.4/32
b1: 159.1.3.3/24
b2: 160.1.3.3/24
b3: 161.1.3.3/24
b4: 162.1.3.3/24
RTU
RTU
10BT
a
b
DSL
DCE Manager Server
DCE Manager Router
b1: 135.1.3.254/24
b2: 135.1.2.1/24
10BT
DSLAM
e1a: 135.1.2.2/24
MCC Card
s1b: 135.1.3.1/24
System Backplane
s1b: 135.1.3.2/24
DSL Card
s1c
s1d
s1e
s1f
IP Interface
e1a: 155.1.3.2/24
156.1.3.2/24
170.1.3.2/24
ISP Router
a: 155.1.2.1/24
b1: 155.1.3.1/24
b16: 170.1.3.1/24
WAN
ISP1
155.1.2.2/16
ISP2
156.1.1.1/16
ISP3
157.1.1.1/16
ISP4
158.1.1.1/16
ISP5
159.1.1.1/16
ISP6
160.1.1.1/16
ISP7
161.1.1.1/16
ISP8
162.1.1.1/16
ISP16
170.1.1.1/16
Notes:
/32 = 255.255.255.255
/24 = 255.255.255.00
/16 = 255.255.00.00
a, b = Interfaces
10BT = 10 BaseT Interface

# Management IP Address Allocation

The primary functionality of the management domain is monitoring and configuring the network. To provide this capability, IP addresses must be allocated for the components that are monitored and configured by the NMS and MCC card.

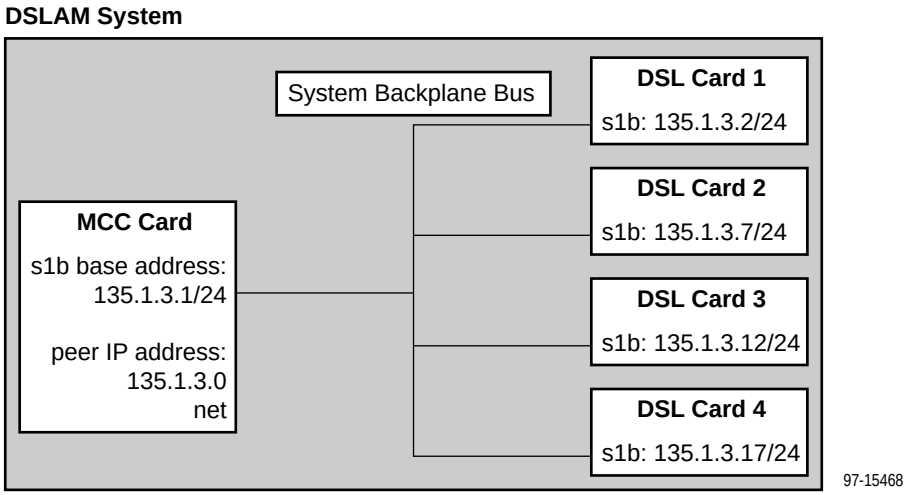
| Component | IP Address Requirement |
|---|---|
| MCC Card | The MCC card must have two IP addresses:<br>■ One IP address for connectivity to the NMS or Router (connecting to the NMS). This address is also known as the Router ID.<br>■ One IP address to communicate to the DSL cards (over the system backplane interface) in the HotWire DSLAM chassis.<br>These two IP addresses must be on separate subnetworks of the NMS domain. That is, they can be on:<br>■ Completely separate networks (e.g., 135.1.0.0/16 and 143.1.0.0/24).<br>■ Completely separate subnets (e.g., 135.1.1.0/24 and 135.1.2.0/24), or<br>■ Subnets of the domain (e.g., 135.1.0.0/16 and 135.1.2.0/24).<br>To configure the MCC card, use the HotWire DSLAM user interface. For step-by-step instructions, see Chapter 4 of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*. |
| DSL Card — Management Domain | Each DSL card must have one management IP address in the same subnetwork as the MCC card's system backplane IP address.<br>To configure the DSL card management IP addresses, use the HotWire DSLAM user interface. For step-by-step instructions, see Chapter 4 of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*. |
| HotWire 5446 RTU — Management Domain | Each RTU must have one management IP address in the same subnetwork as the MCC card's system backplane IP address.<br>NOTE: Since there could be four HotWire 5446 RTU per DSL card and 18 DSL cards per HotWire DSLAM, a maximally-configured system would have 72 HotWire 5446 RTU management IP addresses, and these must be in the same subnetwork as the MCC card's system backplane interface and the 18 DSL cards management IP addresses (total of 91 addresses).<br>To configure the HotWire 5446 RTU management IP addresses, use the HotWire DSLAM user interface. For step-by-step instructions, see Chapter 4 of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*. |

## Peer IP Addresses

Synchronous ports are configured with peer IP addresses. **Peer IP addresses** are used to indicate directly connected systems.

- For the MCC card's s1b (backplane) interface, the peer IP address should be set to indicate the subnet encompassing the DSL cards and RTUs.

  The following illustration shows a HotWire DSLAM system configured with one MCC card and four DSL cards.




  — The IP address of the MCC card's s1b interface is 135.1.3.1.

  — The IP addresses of the DSL card's s1b interfaces are all in the same subnet (135.1.3).

  — Therefore, the directly connected peer subnet is its peer IP address, 135.1.3.0.

- For the DSL card's s1c through s1f interfaces, the peer IP address should be set to indicate the management IP address of the directly connected RTU.

  The peer address for the DSL card is a host route because the peer address identifies a specific RTU. Specifically, the peer address of each DSL card's DSL port is the HotWire 5446 RTU's management IP address. (The peer address is assigned to the RTU through Internet Protocol Control Protocol (IPCP) negotiation.)

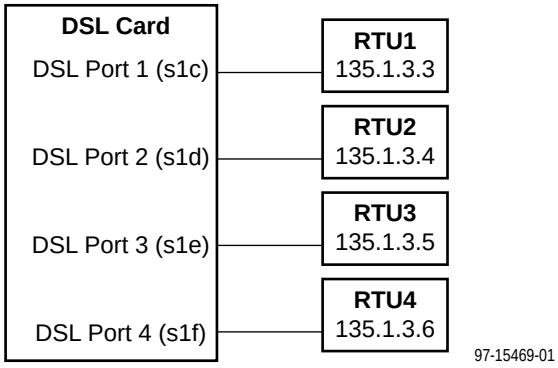
The following illustration shows the DSL card with four RTUs connected to its DSL ports. The peer address for the four DSL card ports are:

— s1c = 135.1.3.3

— s1d = 135.1.3.4

— s1e = 135.1.3.5

— s1f = 135.1.3.6



# Customer IP Address Allocation

Each ISP allocates IP addresses for the components in each customer's network as described below. How the IP addresses are allocated is also noted.

| Component | IP Address Requirement |
|---|---|
| ISP Domain Router | The router that routes ISP traffic to the HotWire DSLAM DSL cards must have one IP address in each customer domain. The router should be multihomed on its LAN port connection to the HotWire DSLAM.<br><br>Since 16 domains are supported per DSL card and there can be 18 DSL cards per HotWire DSLAM, up to 288 ISP IP addresses may be required on the router's interface to support a maximally configured HotWire DSLAM system. However, if efficiently done, only a few would be needed. |
| DSL Card — Customer Domain | Each DSL card can support 16 ISP domains (four for each HotWire 5446 RTU). For each different ISP supported by the DSL card, there must be an IP address in the same domain for the DSL card 10BaseT interface (e1a). Therefore, the total number of DSL card IP addresses required is determined by the number of ISPs supported by the HotWire 5446 RTUs.<br><br>To configure the DSL card management IP addresses, use the HotWire DSLAM user interface. For step-by-step instructions, see Chapter 4 of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*. |
| HotWire 5446 RTU — Customer Domain | Each HotWire 5446 can support four ISP domains. Each HotWire 5446 RTU with an ES in the domain of an ISP must have one customer domain IP address in the same subnetwork.<br><br>There could be:<br><br>■ Four customer domain IP addresses per HotWire 5446 RTU,<br><br>■ Four HotWire 5446 RTU per DSL card, and<br><br>■ 18 DSL cards per HotWire DSLAM.<br><br>This means that a maximally-configured HotWire DSLAM system with 72 HotWire 5446 RTUs could have 288 customer domain IP addresses.<br><br>To configure the HotWire 5446 RTU customer domain IP addresses, use an SNMP application, such as Paradyne's DCE Manager. They are also configurable from a variety of SNMP-based products. |
| End-User System (ES) | Each end user system must have an IP address.<br><br>The IP address is statically assigned by the ISP. |

# Recording Your Configuration Settings

It is recommended that you keep a record of your configuration settings when assigning IP addresses to the devices on your network. Appendix A contains the worksheets to help you record those settings. Store the worksheets for reference, as needed. You may also save your configuration settings on the tFTP server. For information on saving your settings on the tFTP server, see the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

# IP Routing

# 6

## Overview

This chapter presents information regarding the theory behind the configuration of static routes on the HotWire DSLAM, as well as examples. Both standard destination-based routes as well as source-based routes are described.

## Static Routes

The **routing table** stores information about possible destinations for packets being routed through the HotWire DSLAM and identifies the next hop address to which to send the packet. A **static route** is a permanent entry into the routing table that is manually entered. Although the HotWire DSLAM routing table supports both destination-based routing and source-based routing, this section discusses destination-based routing only. (Source-based routing is discussed later in this chapter.)

The routing table is comprised of:

- Configured static routes
- Routes learned by implication of directly connected hosts/networks
- Routes learned by the MCC card from the DSL about its directly connected hosts (RTUs)

With destination-based routing, the destination address of the packet being sent is compared to the destination address entries in the routing table. The destination address could possibly match one or more of three types of addresses in the routing table. It could match a:

- Host route address (that is, a specific destination IP address) e.g., 135.1.3.5, or
- Subnet route, e.g., 135.1.3.0, or
- Network route, e.g., 135.1.0.0

If a match is found for more than one destination address, the order of precedence is:

1. Host route
2. Subnet route
3. Network route
4. Default route

Therefore, the packet is sent to the next-hop address specified for that destination which matches and has the highest precedence.

A packet routed through the HotWire DSLAM that has a destination address not matching any entry in the routing table is dropped unless a default route is specified. If a default route is specified using the conventional address 0.0.0.0 as the destination IP address, the packet is sent to the associated next-hop address.

Since this release of the HotWire DSLAM system uses static addressing, static routes are used to route to the end-user systems. It uses the following routing table form:

*host/subnet/network, next hop, S/D*

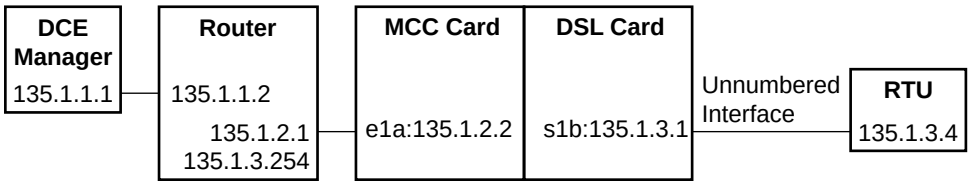
Where:

- The *host/subnet/network* is one of the following:
  - A host address (for example, the specific IP address of an RTU or end-user system), or
  - A subnet or network portion of a destination or source IP address, or
  - The default route, which is defined to be 0.0.0.0.
- The *next hop* is the IP address to which the given datagram should be forwarded. For example, the IP address of the router connected to the LAN or the HotWire RTU.
- *S/D* indicates if the address in the *host/subnet/net* field is a source address or a destination address.

For more information about the routing table, see the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

## MCC Card Static Route Example

The following illustration shows an example of the MCC card routing table.




**MCC Routing Table**

| Host/Net/Subnet | Subnet Mask | Next-Hop Address | S/D (Source/Destination) |
|---|---|---|---|
| 1) 135.1.3.4*<br>2) 0.0.0.0 | 255.255.255.255<br>0.0.0.0 | 135.1.3.1<br>135.1.2.1 | dst (destination)<br>dst (destination) |
| * This entry is automatically generated and does not need to be statically configured. | | | |

97-15478-01

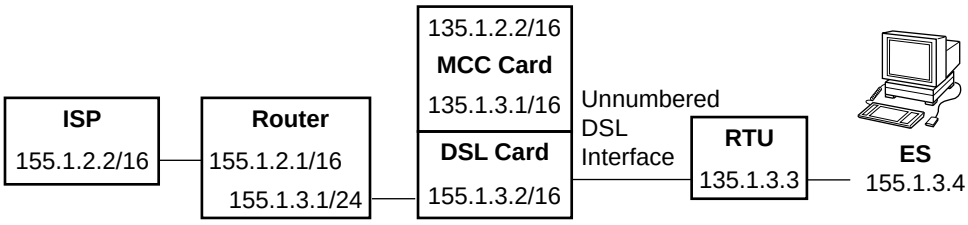
In this example, the IP address of the MCC card's management IP address is 135.1.2.2.

- A packet being routed from the RTU to the NMS is routed using route #2 because no routes for the packet (i.e., destination 135.1.1.1) are specified. Therefore, the default route is used as the next hop address.
- A packet sent by NMS to the RTU is routed using route #1 because the destination IP address of the packet matches the route's Host/Net/Subnet entry (135.1.3.4). Therefore, the next-hop address would be the DSL card (135.1.3.1).

  Note also that the router is multihomed so that both the MCC card's and the DSL card's (management domain) subnetworks appear local (i.e., 135.1.2 and 135.1.3).

## DSL Card Static Route Example

The following illustration shows an example of how static routes configured on a DSL card are used in its routing table:




**DSL Routing Table**

| Host/Net/Subnet | Subnet Mask | Next-Hop Address | S/D (Source/Destination) |
|---|---|---|---|
| 1) 155.1.3.4<br>2) 135.1.1.1<br>3) 0.0.0.0 | 255.255.255.255<br>255.255.255.0<br>0.0.0.0 | 135.1.3.3<br>135.1.3.1<br>155.1.3.1 | dst (destination)<br>dst (destination)<br>dst (destination) |

97-15471-01

In this example:

- The DSL card's Ethernet port is connected to the router's port having an IP address of 155.1.3.1.

  Packets being routed in the upstream direction (to an ISP) would use the third routing table entry, i.e., *Host/Net/Subnet* IP address 0.0.0.0 (by definition) and a *Next Hop* address of 155.1.3.1.

  They would use this route because no other destination would match.

- The management domain IP address of the RTU is 135.1.3.3 and the IP address of the ES is 155.1.3.4. Packets being routed downstream use the first routing table entry, i.e., *Host/Net/Subnet* IP address of 155.1.3.4 and a *Next Hop* address of 135.1.3.3. Note that this is a host route.

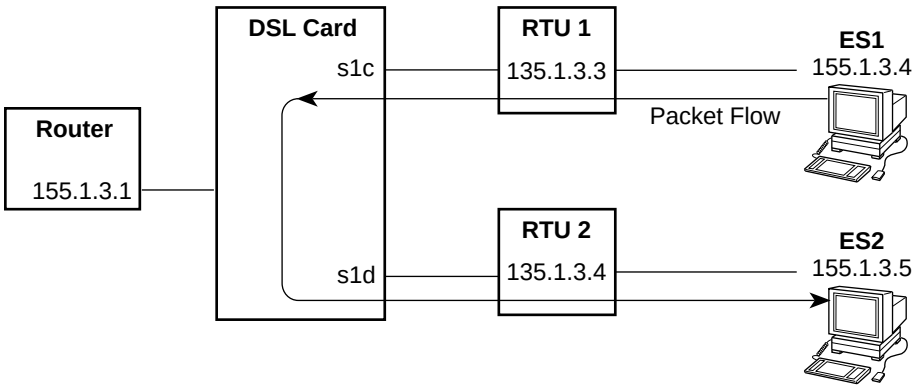
- The second routing table entry is for upstream routing to the NMS via the MCC card. Note that this is a subnet route.

# Source-Based Routing

In addition to destination-based routing, the HotWire DSLAM system also supports source-based routing. **Source-based routing** is a security feature for preventing ES-to-ES routing when they are attached to LANs on different RTUs that are attached to the same DSL card. That is, sourced-based routing can ensure that all upstream traffic within a customer's domain is sent to the ISP.

## Without Source-Based Routing

The following illustration shows, for example, that with destination routing ES1 can send packets to ES2 based on the static route table. That is, when ES1 sends a packet to ES2, the destination route is 159.1.3.4 and the next hop address for this destination is 135.1.3.4 (RTU 2).




**DSL Routing Table**

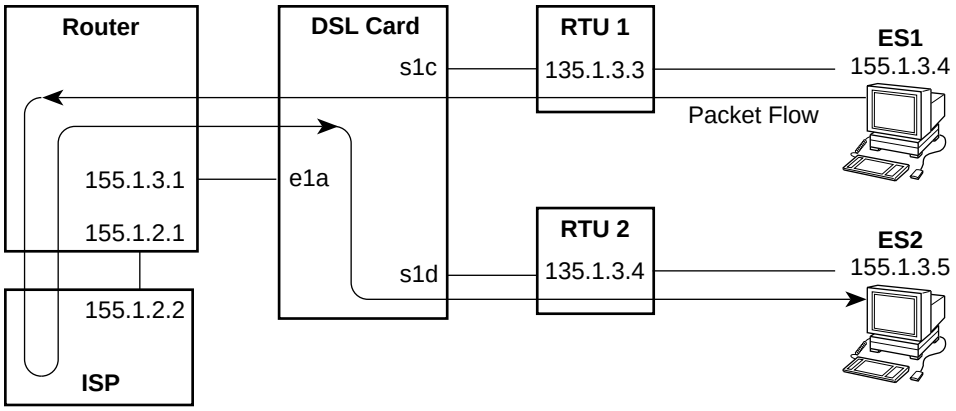
| Host/Net/Subnet | Subnet Mask | Next-Hop Address | S/D (Source/Destination) |
|---|---|---|---|
| 1) 155.1.3.4<br>2) 155.1.3.5<br>3) 0.0.0.0 | 255.255.255.255<br>255.255.255.255<br>0.0.0.0 | 135.1.3.3<br>135.1.3.4<br>155.1.3.1 | dst (destination)<br>dst (destination)<br>dst (destination) |

97-15472-01

## With Source-Based Routing

With source-based routing, the source address of upstream packets sent from an ES are compared to the source address listed in the static route table. If a match is found, the packet is sent to the next-hop address specified for that source address.

The following illustration shows the packet flow when ES1 sends to ES2, and when source-based routes are defined for ES1 and ES2 (indicated by the S/D flag).




**Partial DSL Routing Table**

| Host/Net/Subnet | Subnet Mask | Next-Hop Address | S/D (Source/Destination) |
|---|---|---|---|
| 1) 155.1.3.4<br>2) 155.1.3.5 | 255.255.255.255<br>255.255.255.255 | 155.1.3.1<br>155.1.3.1 | src (source)<br>src (source) |

97-15473-01

Upstream packets from ES1 (and ES2) are sent to 155.1.3.1, where in turn the router would forward them to the ISP. Downstream packets from the ISP are sent to ES2.

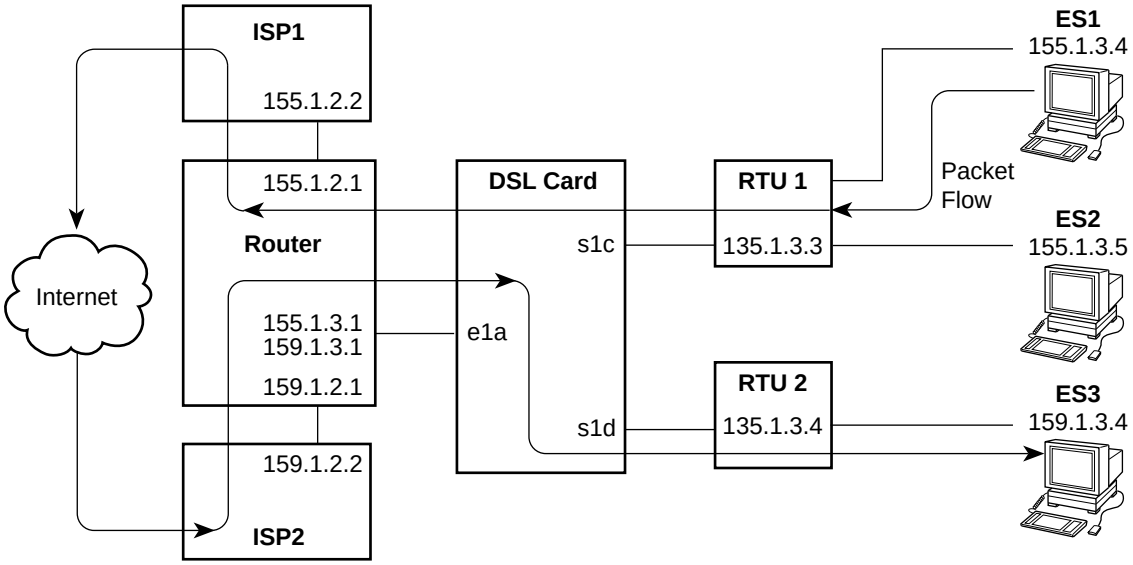
For upstream packets only (i.e., packets arriving over the DSL ports), the order of routing precedence is:

- Source host route
- Source subnet route
- Source network route
- Destination host route
- Destination subnet route
- Destination network route
- Default route

**NOTE:**

When using source routing, do not use the default route.

The following illustration shows the packet flow when ES1 sends to ES3, ES1 and ES3 are in different customer domains, and source-based routes are defined for ES1 and ES2 (indicated by the S/D flag).




**Partial DSL Routing Table**

| Host/Net/Subnet | Subnet Mask | Next-Hop Address | S/D (Source/Destination) |
|---|---|---|---|
| 1) 155.1.3.4<br>2) 155.1.3.5<br>3) 159.1.3.4 | 255.255.255.255<br>255.255.255.255<br>255.255.255.255 | 155.1.3.1<br>155.1.3.1<br>159.1.3.1 | src (source)<br>src (source)<br>src (source) |

97-15560

# IP Filtering

# 7

## Overview

A filter is a useful mechanism. It can be used to secure a network by implementing security rules (policies). You can use a filter to prevent unauthorized network access without making authorized access difficult.

By default, filtering is not active on the HotWire DSLAM system. However, you can enable filtering to selectively filter source or destination packets being routed through the MCC or DSL cards. Appendix B, *IP Filtering Configuration Worksheets*, provides worksheets to help you plan and record your filter configurations.

This chapter provides an overview of packet filters and describes why you may want to set filters on your network.

## What is a Filter?

An **IP filter** is a rule (or set of rules) that is applied to a specific interface to indicate whether a packet can be forwarded or discarded.

A filter works by successively applying the rules to the information obtained from the packet header until a match is found. The filter then performs the action specified by the rule on that packet, which can be either to forward or discard the packet. The filter does not keep any state or context, and the decision is made based only on the packet contents.

You can create the following filter types:

- An **input filter** to prevent packets entering the DSL card through a specified interface from being forwarded. You may want to set up filtering on input to protect against address spoofing. Use the IP Network screen (*Configuration* → *Interfaces* → *IP Network*) to specify whether or not you want to use an input filter.
- An **output filter** to prevent packets from going out of the DSL card through a specified interface. Use the IP Network screen (*Configuration* → *Interfaces* → *IP Network*) to specify whether or not you want to use an output filter.

**NOTE:**

You can specify an input filter for one interface and an output filter for another interface. Do not, however, specify an input filter and an output filter for the same interface.

For each filter type, you must set up one or more of the following rule types on the IP Filter Configuration screen (*Configuration → IP Router → IP Router Filters*):

- A **network address rule type** to discard or forward packets/traffic from a specified network or a segment of the network. This rule type can also be used to enhance security by allowing access only to certain networks. The IP address and subnet mask specified in the `Destination address` and `Destination address mask` fields, or the `Source address` and `Source address mask` fields of the IP Filter Configuration screen are compared to the destination/source address contained in the IP header of the packet.
- A **host address rule type** to discard or forward packets/traffic from a specified host. This rule type can also be used to enhance security by allowing access only to certain hosts. The IP address and subnet mask specified in the `Destination address` and `Destination address mask` fields, or the `Source address` and `Source address mask` fields of the IP Filter Configuration screen are compared to the destination/source address contained in the IP header of the packet.
- A **socket address rule type** to limit certain applications. This rule type is used primarily when filtering TCP or UDP packets, and may be used in conjunction with a network address rule type or a host address rule type. The destination (socket) port number specified in the `Destination Port No.` field and source (socket) port number specified in the `Source Port No.` field of the IP Filter Configuration screen are compared to the destination and source port numbers in the TCP or UDP header of the packet.

**NOTE:**

If both the source and destination port numbers are 0s (zeros), the system filters ICMP packets in addition to the packet types defined in the rule.

In this release, up to 33 rules can be configured for each filter. By default, if you do not specify rules, the system will forward packets.

For detailed information on the IP Filter Configuration screen and the IP Network screen, see Chapters 5 and 6 of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

# Security Advantages

Filtering provides security advantages on LANs as described in the following subsections.

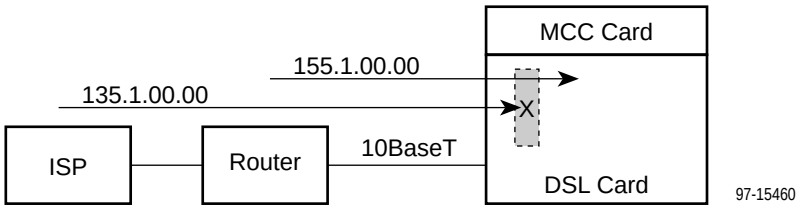
**NOTE:**

All upstream traffic from an ES is forwarded by the HotWire 5446 RTU to the DSL card unless it is addressed to another ES (in the same subnet) on the same LAN.

## Management Traffic Leakage

Filtering can be used to prevent unwanted traffic from leaking into the management domain. That is, filtering prevents ISP packets with management IP destinations from being accepted for local delivery or routing.

For example, if the ISP network is 155.1.00.00 and the management network is 135.1.00.00, filters can be defined that would prevent any traffic entering from the 10BaseT port from being forwarded to the 135.1.00.00 network through the DSL card.




**NOTE:**

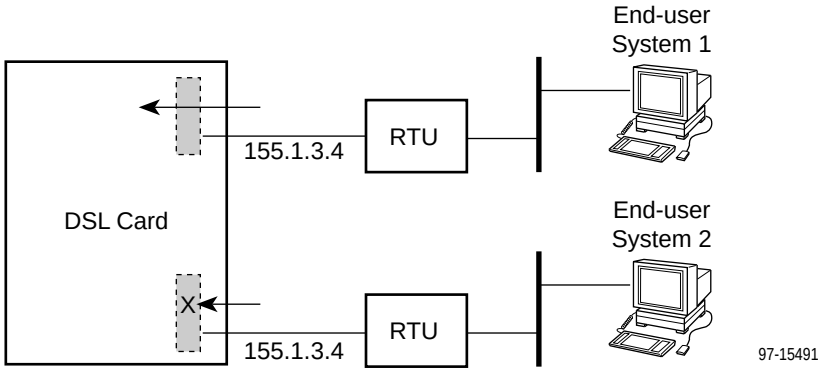
Filters reduce packet throughput.

For instructions on how to set filters to prevent unwanted traffic from leaking into the management domain, see Chapter 5 of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

## Service Security

Filtering on the upstream DSL ports can be used to ensure that only end-user systems with valid IP addresses are able to route traffic to the ISP domain. That is, filtering would block traffic from being routed upstream by another end-user system that spoofs (attempts to gain access to another system by posing as an authorized user) an IP address of an end-user system connected to a different HotWire 5446 RTU.

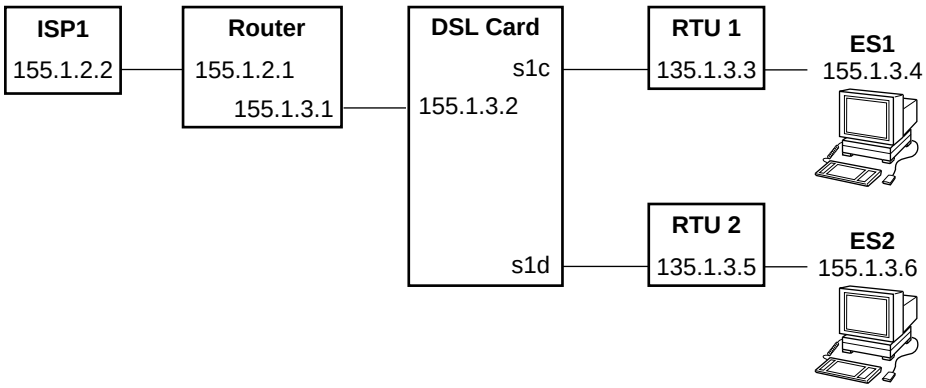
The following illustration is an example of this type of filtering:




For information on how to set filters on the upstream DSL ports, see Chapters 5 and 6 of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

# Service Security Filtering Scenario

The following is an example of filtering to ensure service security:



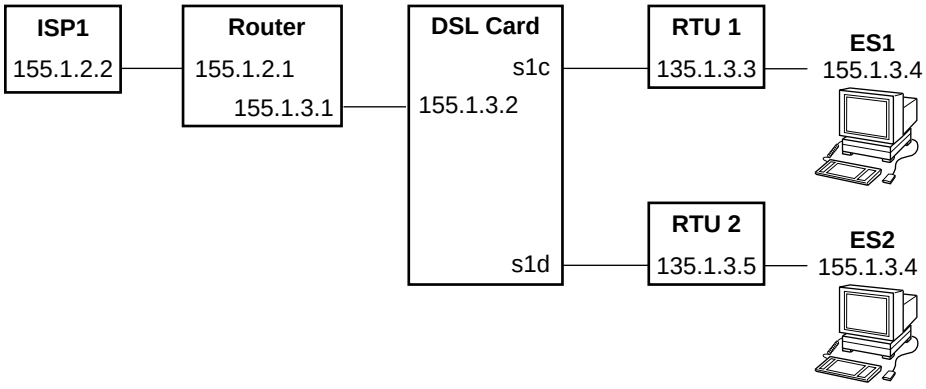

**DSL Routing Table**

| Host/Net/Subnet | Subnet Mask | Next-Hop Address | S/D (Source/Destination) |
|---|---|---|---|
| 1) 155.1.3.4<br>2) 155.1.3.4<br>3) 155.1.3.6<br>4) 155.1.3.6 | 255.255.255.255<br>255.255.255.255<br>255.255.255.255<br>255.255.255.255 | 155.1.3.1<br>135.1.3.3<br>155.1.3.1<br>135.1.3.5 | src (source)<br>dst (destination)<br>src (source)<br>dst (destination) |

97-15476-01

The RTU forwards upstream any traffic on its LAN interface for which it does not know the host.

In the following illustration, ES2 spoofs ES1's IP address (that is, ES2 assumes ES1's IP address of 155.1.3.4):




*ES2 spoofing ES1's address*

**DSL Routing Table**

| Host/Net/Subnet | Subnet Mask | Next-Hop Address | S/D (Source/Destination) |
|---|---|---|---|
| 1) 155.1.3.4<br>2) 155.1.3.4<br>3) 155.1.3.6<br>4) 155.1.3.6 | 255.255.255.255<br>255.255.255.255<br>255.255.255.255<br>255.255.255.255 | 155.1.3.1<br>135.1.3.3<br>155.1.3.1<br>135.1.3.5 | src (source)<br>dst (destination)<br>src (source)<br>dst (destination) |

97-15477-01

With no input filtering on the DSL ports, ES2 can successfully send traffic to the ISP identifying itself as ES1 (155.1.3.4).

Now, consider that the following filter rules are applied to s1d:

| **IP Address** | **Subnet Mask** | **Source/Destination** | **Action** |
|---|---|---|---|
| 155.1.3.6 | 255.255.255.255 | Source | Forward |
| Default | — | — | Discard |

With these filter rules active on s1d, when ES2 tries to send packets to ISP1, the filter on the DSL card blocks the packets from being forwarded, because only packets with a source IP address of 155.1.3.6 are forwarded.

# SNMP Agent

# 8

## Overview

The Simple Network Management Protocol (SNMP) is an application-level protocol used in network management. A Network Management System (NMS), such as Paradyne's DCE Manager, communicates to an SNMP agent via SNMP in order to obtain (get) specific parameters or variables within control of the SNMP agent. Note that the set capability will be supported in a future release of the HotWire DSLAM software.

When DCE Manager is configured properly, it can communicate with the HotWire DSLAM SNMP agent. Almost all communications between the DCE Manager and the HotWire DSLAM SNMP agent originate with a request message from the DCE Manager to the HotWire DSLAM. When the DSLAM receives the request, the HotWire DSLAM SNMP agent processes the request message and transmits a response (positive or negative) message back to the DCE Manager. When certain significant events occur within the SNMP agent, this can result in transmission of unprompted SNMP trap messages to the DCE Manager. (Note that the HotWire DSLAM SNMP agent is SNMP Version 1 (V1) compliant with community-based management.)

This chapter describes what you need to know to configure the SNMP agent within the HotWire DSLAM. This chapter does not, however, describe the procedures on how to configure the SNMP agent. For those procedures, see the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

## MIB Compliance

Various pieces of configuration, status, and statistical data within the HotWire DSLAM SNMP agent form a database of information that is accessible from the DCE Manager. This collection of information is called a Management Information Base (MIB). The basic definitions of the content of an SNMP agent's MIB are defined within various Internet Request for Comments (RFC) documents.

An HP OpenView MIB browser requires the operator to load the appropriate MIB files into its database before it can manage the HotWire DSLAM network. However, when using DCE Manager, the appropriate MIB files are loaded automatically. For more information about DCE Manager, see the *DCE Manager for HP OpenView for Widows User's Guide* or the *DCE Manager for HP OpenView User's Guide*.

The HotWire DSLAM supports the following MIBs:

- MIB II — System Group (described in RFC 1213)
- MIB II — ICMP Group (described in RFC 1213)
- MIB II — UDP Group (described in RFC 1213)
- MIB II — Transmission Group (described in RFC 1213)
- MIB II — SNMP Group (described in RFC 1213)
- MIB II — Definitions of Managed Objects for the Ethernet-like Interface Types (described in RFC 1398)
- MIB II — Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol (described in RFC 1471)
- MIB II — Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol (described in RFC 1473)
- MIB II — Evolution of Interfaces Group (described in RFC 1573)
- MIB II — Ethernet Interface MIB (described in RFC 1643)
- Entity MIB (described in RFC 2037)
- Paradyne DSL Enterprise MIBs:
  - — HotWire System MIB (hot_sys.mib)
  - — HotWire xDSL MIB (hot_xdsl.mib)
  - — Security MIB (devSecurity.mib)
  - — Device Health and Status MIB (devHealthAndStatus.mib)

# Supported Traps

SNMP defines six basic or standard traps. These messages are identified with a value of 0 through 5 within the generic-trap field of the trap message. (Note that the HotWire DSLAM SNMP agent does not support trap messages with a value of 5.) The specific-trap field of standard trap messages is set to 0 (zero). The specific-trap field of enterprise-specific messages defines the trap.

The HotWire DSLAM SNMP agent supports generation of the following standard trap messages (specific-trap=0):

- **coldStart(0)**. The sending SNMP agent reinitializes itself such that the agent's configuration may be altered.
- **warmstart(1)**. The sending SNMP agent is reinitialized without altering the agent's configuration.
- **linkDown(2)**. A link on the sending SNMP agent is no longer operational.
- **linkUp(3)**. A link on the sending SNMP agent has become operational.

- **authenticationFailure(4)**. The sending SNMP agent has received an SNMP message specifying a community name which it does not recognize, or requesting an action not permitted for the specified community.

There are additional supported traps, which can be found in the Paradyne DSL Enterprise MIBs. See the MIBs for a complete list of traps.

The generation of SNMP trap messages can be selectively enabled per configured community. Additionally, the authenticationFailure trap can be selectively enabled for all configured communities that have traps enabled. In other words, each community can give all trap messages (either enabled or disabled). If any communities have the generation of trap messages enabled, then the generation of authenticationFailure traps is determined by the state of the global authenticationFailure switch.

# General SNMP Agent Configuration

Depending on your specific network configuration, various aspects of the HotWire DSLAM SNMP agent may need to be configured. For example, you may want to set up your system to send SNMP traps to a specific SNMP NMS manager. The HotWire DSLAM system provides four default community names (two read/write community names and two read-only community names) per MCC or DSL card. These community names are similar to passwords. Make sure that the SNMP NMS manager that will receive SNMP trap messages knows and uses the correct community name, as specified on the HotWire DSLAM. You can change the default community names to match the name of the SNMP NMS manager. Without the correct community name, the NMS manager will not be able to communicate with the DSLAM.

As a minimum configuration, you must do the following on the SNMP Communities/Traps screen:

- Assign an SNMP NMS manager to a community by specifying the SNMP NMS manager's IP address to a specific community name. (Ensure that the SNMP NMS manager uses the same community name configured in the HotWire DSLAM.) You can specify up to three SNMP NMS managers for each community name.
- Configure the generation of trap messages.
- Enable/Disable the generation of authenticationFailure trap messages.

Additionally, you can configure logical entities. Logical entities can be used to provide various management populations with different levels of management access to the HotWire DSLAM SNMP agent. These configurations provide a system-wide view of the SNMP agent. Use the Configure SNMP Logical Entity Table screens to configure access logical entities.

For detailed information about the various SNMP Agent screens mentioned in this chapter, see Chapters 5 and 6 of the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*. Also Appendix C, *SNMP Configuration Worksheets*, provides worksheets to help you plan and record your SNMP configurations.

# Packet Walk-Throughs

# 9

## Overview

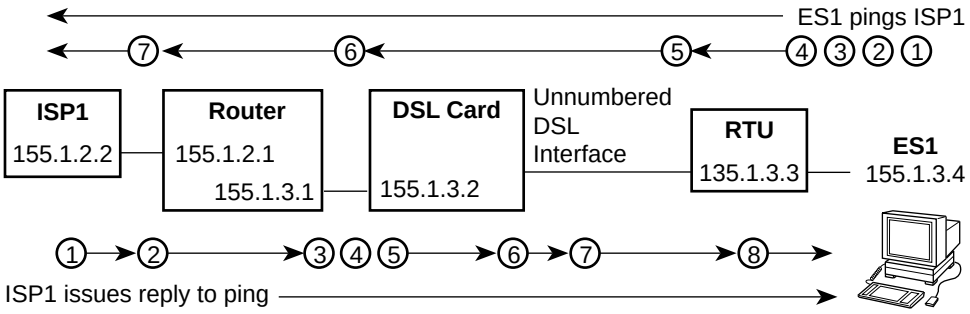
This chapter provides examples of how data packets are routed through the customer and management domains.

## Customer Packet Walk-Through

To examine how data packets flow through the customer domain, an example of ES1 issuing a ping to ISP1 will be used. The following assumptions are made:

- A host route entry has been configured in the HotWire 5446 RTU for ES1
- A source domain IP entry exists for the HotWire 5446 RTU
- A static route exists between the DSL card and the HotWire 5446 RTU
- Upstream filtering is disabled

The following illustration shows how data packets flow through the customer domain. In this illustration ES1 is connected to the same LAN as the HotWire 5446 RTU.




**Partial DSL Routing Table**

| Host/Net/Subnet | Subnet Mask | Next-Hop Address | S/D (Source/Destination) |
|---|---|---|---|
| 1) 155.1.3.4<br>2) 155.1.3.4 | 255.255.255.255<br>255.255.255.255 | 155.1.3.1<br>135.1.3.3 | src (source)<br>dst (destination) |

97-15474-01

When ES1 pings ISP1:

1. ES originates a packet addressed to 155.1.2.2. Because they are both on the 155.1 network, ES1 ARPs to map ISP1's IP address into a MAC address.
2. The RTU receives the broadcast ARP request from ES1.
3. The RTU replies to the ARP request with its own MAC address (proxy ARP).
4. After ES1 receives the ARP reply, it sends the packet to the MAC address of the RTU.
5. Upon receiving this packet, the RTU forwards it to the DSL card over its DSL interface.
6. When the DSL card receives this packet, the DSL card consults its routing table to determine how to route the packet. Since a source route is defined for ES1 (route #1), the DSL card forwards the packet to the router (151.1.3.1), which is the next-hop.
7. The router then forwards the packet to ISP1.

ISP1 then issues a reply to the ping.

1. The ISP sends the ping reply packet addressed to 155.1.3.4.
2. By normal means, the packet arrives at the router.
3. Because the router has an interface with an address 155.1.3.1 (on 155.1.3 subnet) it ARPs for 155.1.3.4.
4. Because the DSL card has a host route (marked PA=y) for 155.1.3.2, it responds to the ARP request with its own MAC address (proxy ARP).
5. Then, the ping reply is sent directly to the DSL card.
6. The DSL card then consults its routing table to identify the next hop to forward the packet. Since a host route is defined for ES1 (route #2), the RTU 135.1.3.3 is used as the next hop.

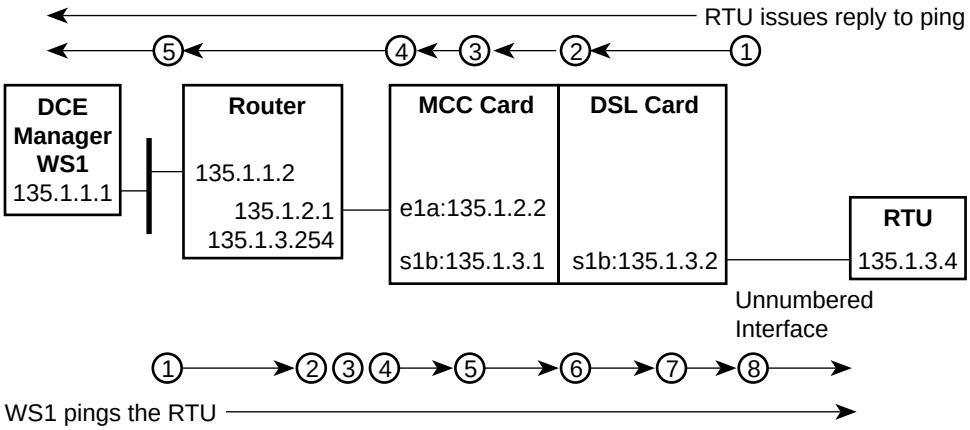
7. The DSL card then forwards the packet over the DSL port to that RTU.
8. Upon receiving the packet, the RTU forwards the packet to its 10BaseT port because it has a host route for ES1.

# Management Packet Walk-Through

To examine how data packets flow through the management domain, an example of the DCE Manager workstation 1 (WS1) performing a ping to the HotWire 5446 RTU will be used. The following is assumed:

- A host route to the RTU (135.1.3.4) exists on the MCC card. (This is generated automatically.)
- A static route to WS1 (135.1.1.1) is configured on the DSL card.

In the following illustration, WS1 is connected to the same LAN as the NMS.




**MCC Routing Table**

| Host/Net/Subnet | Subnet Mask | Next-Hop Address | S/D (Source/Destination) |
|---|---|---|---|
| 1) 135.1.3.4<br>2) 0.0.0.0 | 255.255.255.255<br>0.0.0.0 | 135.1.3.2<br>135.1.2.1 | dst (destination)<br>dst (destination) |

**Partial DSL Routing Table**

| Host/Net/Subnet | Subnet Mask | Next-Hop Address | S/D (Source/Destination) |
|---|---|---|---|
| 1) 135.1.2.0<br>2) 135.1.1.0 | 255.255.255.0<br>255.255.255.0 | 135.1.3.1<br>135.1.3.1 | dst (destination)<br>dst (destination) |

97-15479-01

When WS1 pings a HotWire 5446 RTU:

1. The packet addressed to 135.1.3.4 is routed to the router by normal means.
2. The router then does an ARP request for the RTU because the router's IP address of 135.1.3.254 is on the same subnetwork as the RTU (with an IP address of 135.1.3.4).

   Note that the router's interface to the MCC is multihomed (i.e., it has two IP addresses (135.1.2.1 and 135.1.3.254) assigned to the one interface).
3. The MCC does an ARP reply with its own MAC address (proxy ARP).
4. The router then forwards the ping packet to the MCC card.
5. Upon receiving the ping, the MCC card consults its routing table to identify to which DSL card to forward the ping.

   In this case, route #1 contains a host route for 135.1.3.4 with a next hop of DSL 135.1.3.2.
6. The ping request is then forwarded to the DSL card from the MCC card's *s1b* interface to the DSL card's *s1b* interface (which is over the DSLAM system backplane).
7. The DSL card knows that 135.1.3.4 is directly connected over s1c (one of the DSL card's DSL ports).
8. The DSL card then forwards the ping to the RTU over s1c.

The HotWire 5446 RTU then issues a ping reply to IP address 135.1.1.1.

1. The RTU forwards the ping reply to the DSL card.
2. The DSL card consults its routing table to identify how to forward the reply. Route #2 is used because the destination address (135.1.1.1) is the 135.1.1 subnet. Therefore, the next-hop address is the MCC card's *s1b* interface (135.1.3.1).
3. Similarly, upon receiving the packet, the MCC card consults its routing table to identify how to forward the packet. Since the destination IP address of the ping is WS1 (135.1.1.1) and this does not match any entry in the route table, the next-hop IP address (135.1.2.1) of the default route is used.
4. The MCC card then forwards the packet to its 10BaseT interface to the router.
5. The router forwards the packet toward WS1 by normal means.

# Network Configuration Worksheets

# A

## Overview

This appendix summarizes the mandatory minimum configuration steps and provides worksheets to assist you in preparing for the configuration of your HotWire DSLAM network. Use the worksheets to record configuration settings such as IP addresses and subnet masks for the MCC card, DSL cards, and RTUs. After the worksheets are completed, you can then configure your network with the assigned settings.

These worksheets are based on the network model and theories described in this guide. They map the network theories to the HotWire user interface screens. For an explanation of the network model and theories, review the chapters in this guide. For specific information about the user interface screens and fields, see the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

## Summarizing the Network Configuration

In summary, to configure the network:

- The management domain and customer domain IP addresses and static routes are assigned to the HotWire DSLAM system using the HotWire software.
- The HotWire 5446 RTU's management IP address is also assigned from the HotWire software.
- The customer domain IP addresses and host routes on the HotWire 5446 RTU are assigned by using an SNMP application, such as Paradyne's DCE Manager or by using a MIB browser.
- The IP addresses of the end-user systems are assigned by the ISP.

# Management Domain Configuration Worksheets

For the management domain, configure the MCC card, DSL cards, and HotWire 5446 RTUs as follows:

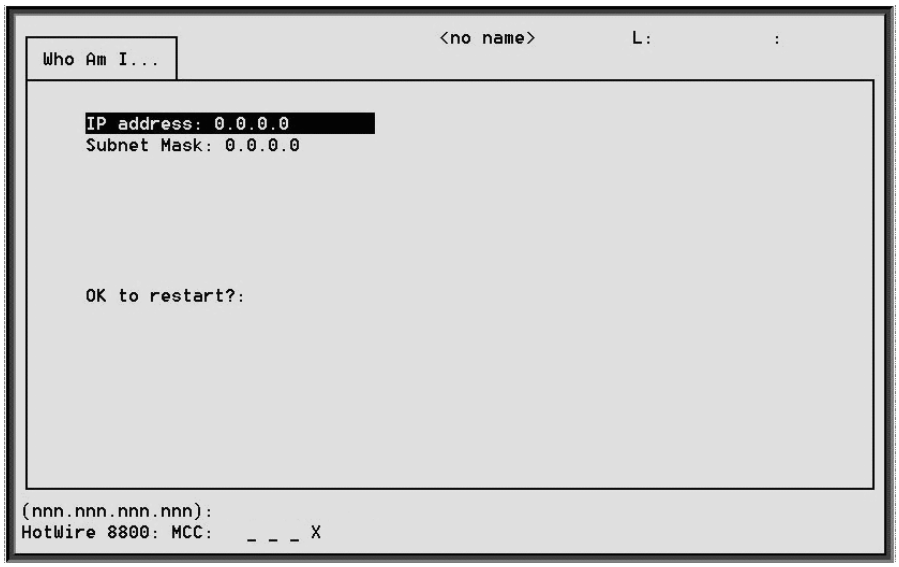
| Perform this task . . . | On this screen . . . | To access screen . . . |
|---|---|---|
| 1. Assign an IP address to the MCC card. | Who Am I screen | Power on the HotWire DSLAM system.<br>The system displays the Who Am I screen. |
| 2. Assign an IP address to the backplane (s1b) on the MCC card. | (HotWire – MCC) IP Network screen | From the HotWire – MCC menu, select: *Configuration → Interfaces → IP Network* |
| 3. Assign IP addresses to the DSL cards. | (HotWire – MCC) Configure DSL IP Addr screen | From the HotWire – MCC menu, select: *Configuration → DSL Cards → Set IP Address* |
| 4. Create default route. | (HotWire – MCC) Static Routes screen | From the HotWire – MCC menu, select: *Configuration → IP Router → Static Routes* |
| 5. Reset the MCC card. | (HotWire – MCC) Card Reset screen | From the HotWire – MCC menu, select: *Configuration → Card Status → Card Reset* |
| 6. Assign an IP address within the management subnetwork for each HotWire 5446 RTU. | (HotWire – DSL) IP Network screen | From the HotWire – DSL menu, select: *Configuration → Interfaces → IP Network* |
| 7. Configure a static route to the NMS (on each DSL card). | (HotWire – DSL) Static Routes screen | From the HotWire – DSL menu, select: *Configuration → IP Router → Static Routes* |

Use the worksheets in the following sections to record your network configuration settings. Photocopy the worksheets as needed.

## Assign an IP Address to the MCC Card

On the Who Am I screen, assign an IP address to the MCC card.

| Access the . . . | By . . . |
|---|---|
| Who Am I screen | Powering on the HotWire DSLAM system. |




| Who Am I Screen | |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. Enter the IP address to the MCC card (e1a) at the `(nnn.nnn.nnn.nnn):` prompt. | IP Address = |
| 2. Enter the subnet mask at the `(nnn.nnn.nnn.nnn):` prompt.<br>Note that the system automatically calculates the subnet mask. Press Return to accept the default value or enter a new value at the prompt. | Subnet Mask = |
| 3. Reboot the system by typing **yes** at the `yes/no:` prompt, when the system highlights `OK to restart?.` | |

**NOTE:**

To continue configuring the management domain, you must select the MCC card.

After the system reboots, press Return to display the HotWire Chassis menu.

— From the HotWire Chassis menu, select Card Selection.

The Card Selection screen appears.

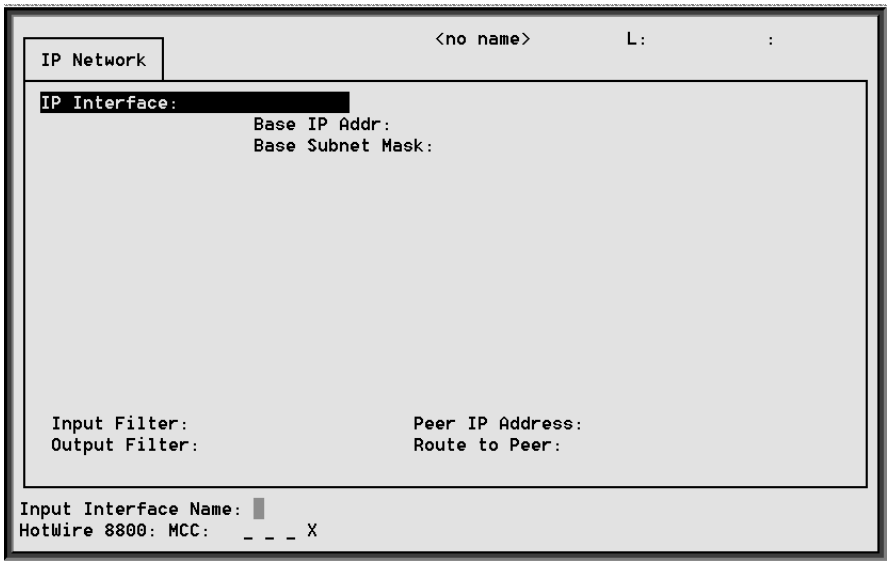
— At the `Goto Card (MCC or DSLnn):` prompt, enter **MCC** and press Return.

The HotWire – MCC menu appears.

## Assign an IP Address to the Backplane (s1b)

On the IP Network screen, assign an IP address to the backplane (s1b).

| Access the . . . | By . . . |
|---|---|
| IP Network screen | Selecting *Configuration* → *Interfaces* → *IP Network* from the HotWire – MCC menu. |

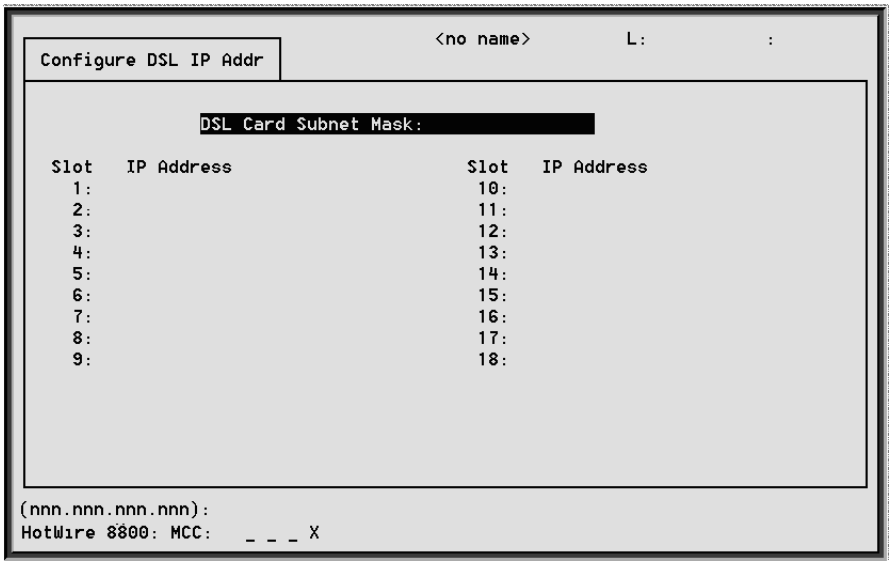



| IP Network Screen | A-C-B |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. Enter the interface name at the `Input Interface Name:` prompt. | IP Interface = **s1b** |
| 2. Enter the base IP address at the `(nnn.nnn.nnn.nnn):` prompt. | Base IP Addr = |
| 3. Enter the base subnet mask at the `(nnn.nnn.nnn.nnn):` prompt. | Base Subnet Mask = |
| 4. Enter the peer IP address at the `(nnn.nnn.nnn.nnn)or address-pool:` prompt. | Peer IP Address = |
| 5. Enter route type **NET** (for network) at the `Route to peer (host/net):` prompt. | Route to Peer= **NET** |

## Assign IP Addresses to the DSL Cards

On the Configure DSL IP Addr screen, assign an IP address to each DSL card in the system.

| **Access the . . .** | **By . . .** |
|---|---|
| Configure DSL IP Addr screen | Selecting *Configuration* → *DSL Cards* → *Set IP Address* from the HotWire – MCC menu. |

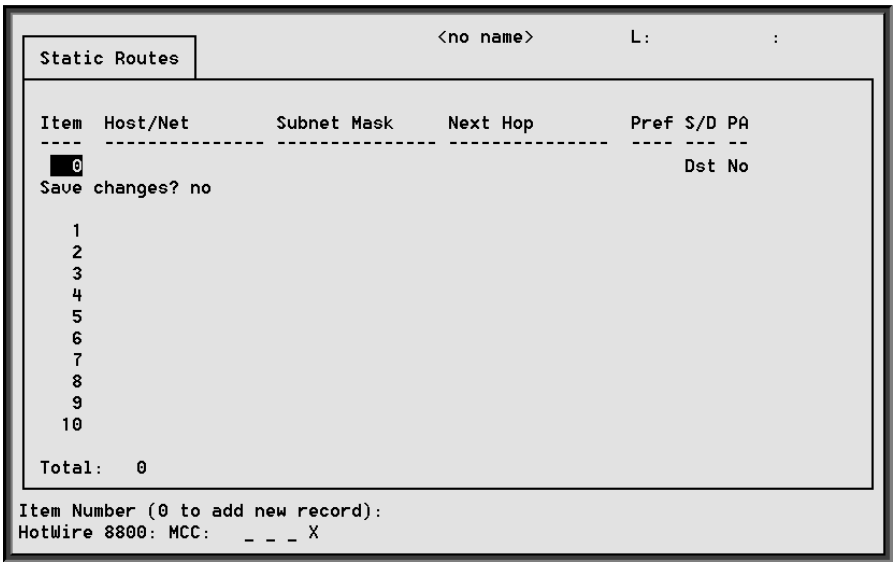


| **Configure DSL IP Addr Screen** | **A-G-A** |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. Enter the DSL card subnet mask at the `(nnn.nnn.nnn.nnn):` prompt.<br>This is the subnet mask for the backplane (s1b) management subnet. | DSL Card Subnet Mask = |
| 2. Enter the IP address for each DSL card in the system. Select the appropriate slot number by using the arrow keys to move from one field to another.<br>Once the slot number is selected, enter the IP address for that DSL card at the `(nnn.nnn.nnn.nnn):` prompt. | Slot 1 IP Address =<br>Slot 2 IP Address =<br>Slot 3 IP Address =<br>Slot 4 IP Address =<br>Slot 5 IP Address =<br>Slot 6 IP Address =<br>Slot 7 IP Address =<br>Slot 8 IP Address =<br>Slot 9 IP Address =<br>Slot 10 IP Address =<br>Slot 11 IP Address =<br>Slot 12 IP Address =<br>Slot 13 IP Address =<br>Slot 14 IP Address =<br>Slot 15 IP Address =<br>Slot 16 IP Address =<br>Slot 17 IP Address =<br>Slot 18 IP Address = |

## Create a Default Route

On the Static Routes screen, create a default route to the management domain next hop router. This default route will be used when no other routes in the routing table apply.

| Access the . . . | By . . . |
|---|---|
| Static Routes screen | Selecting *Configuration* → *IP Router* → *Static Routes* from the HotWire – MCC menu. |

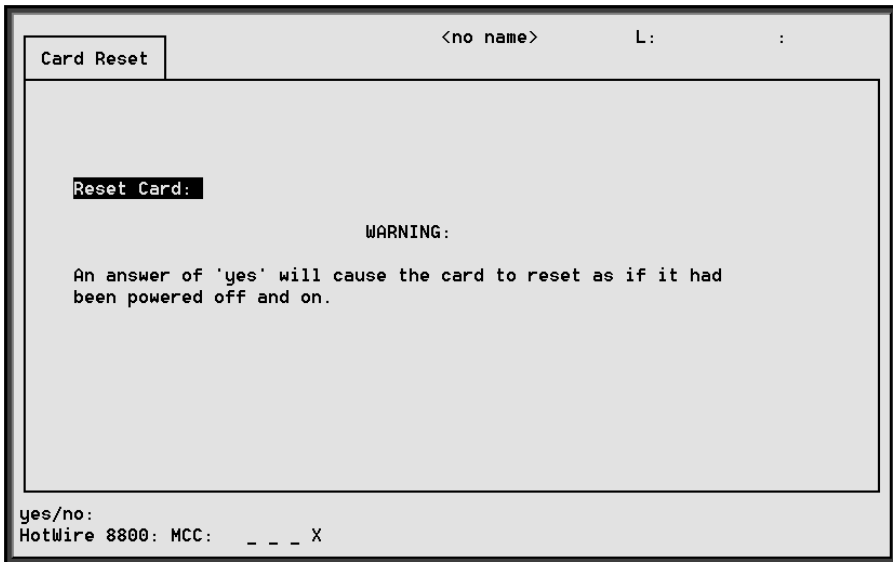



| Static Routes Screen | A-E-A |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. Enter **0** or press Return at the `Item Number (0 to add new record):` prompt to add a new record. | |
| 2. Enter **0.0.0.0** at the `Destination (or space to delete route):` prompt. | Host/Net = **0.0.0.0** |
| 3. Press Return at the `Subnet:(nnn.nnn.nnn.nnn):` prompt. | Subnet Mask = **0.0.0.0** |
| 4. Enter the IP address of the default route to the management domain next hop address at the Next Hop `IP Address (nnn.nnn.nnn.nnn):` prompt. | Next Hop = |

| **Static Routes Screen** | **A-E-A** |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 5. Enter **1** at the `Input Number:` prompt to specify the preference for this route.<br>1 has the highest preference. The greater the number the lower the preference. | Pref= **1** |
| 6. Enter **dst** or press Return at the `Source (Src)/ Destination(dst):` prompt. | S/D= **dst** |
| 7. Enter **no** or press Return at the `yes/no:` prompt to keep the NO value under the PA (proxy ARP) column. | PA= **no** |
| 8. When the system highlights `Save Changes?`, enter yes at the `yes/no:` prompt. | |

## Reset the MCC Card

After configuring the MCC card for the management domain, reset the card to install the configuration setting. On the Card Reset screen (*Configuration → Card Status → Card Reset)*, reset the MCC card by entering **yes** at the `yes/no:` prompt.




### NOTE:

After resetting the MCC card, select a DSL card to continue with the management domain configuration. To select a DSL card:

— Press Return to display the top-level menu (HotWire Chassis menu).

— Select `Card Selection` from the HotWire Chassis menu.

The Card Selection screen appears.

— Verify that the DSL card you want to configure appears on the Card Status screen.

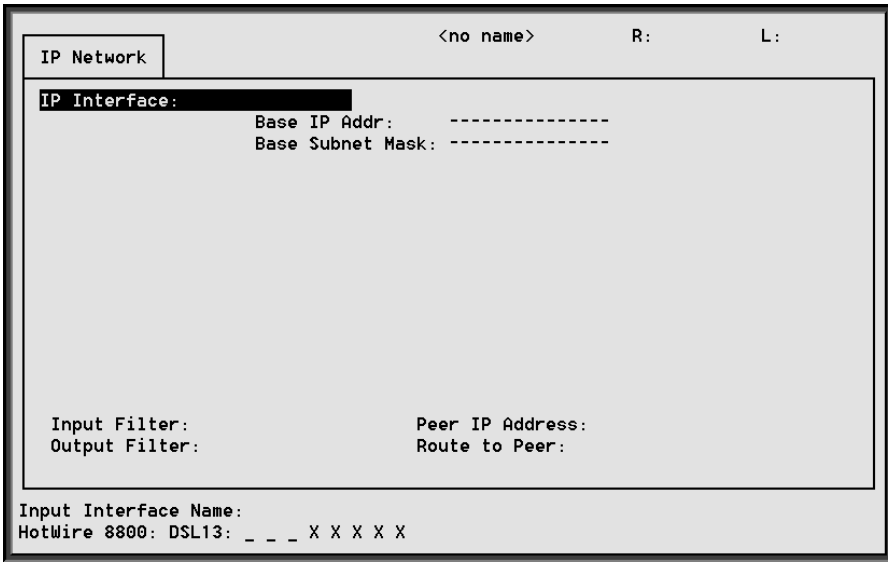
— At the `Goto Card (MCC or DSLnn):` prompt, enter **DSL** and the number of the slot. Then, press Return. For example, if you want to configure the DSL card in slot 13, enter **DSL13**.

The HotWire – DSL menu appears.

## Configure the HotWire 5446 RTU Management Domain IP Addresses

On the IP Network screen, configure the HotWire 5446 RTU IP addresses on each DSL card, which are the RTU's management domain IP addresses.

| Access the . . . | By . . . |
|---|---|
| IP Network screen | Selecting *Configuration* → *Interfaces* → *IP Network* from the HotWire – DSL menu. |



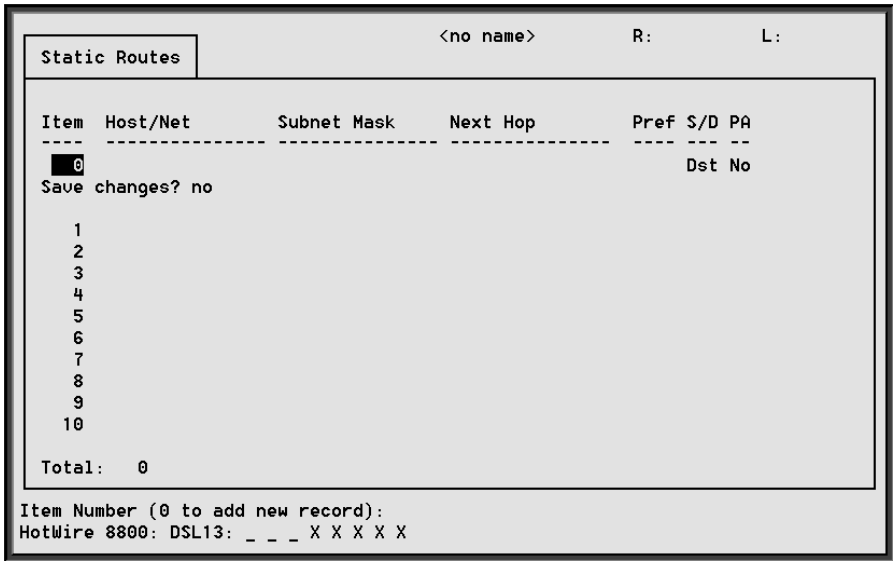

| IP Network Screen | A-C-B |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| **For DSL port 1 (s1c):** | |
| 1. Enter the interface name at the `Input Interface Name:` prompt. | IP Interface = **s1c** |
| 2. Enter the peer IP address at the `(nnn.nnn.nnn.nnn)or address-pool:` prompt. | Peer IP Address = |
| 3. Enter route type **HOST** at the `Route to peer (host/net):` prompt. | Route to Peer= **HOST** |
| **For DSL port 2 (s1d):** | |
| 1. Enter the interface name at the `Input Interface Name:` prompt. | IP Interface = **s1d** |
| 2. Enter the peer IP address at the `(nnn.nnn.nnn.nnn)or address-pool:` prompt. | Peer IP Address = |

| IP Network Screen | A-C-B |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 3. Enter route type **HOST** at the `Route to peer (host/net):` prompt. | Route to Peer= **HOST** |
| **For DSL port 3 (s1e):** | |
| 1. Enter the interface name at the `Input Interface Name:` prompt. | IP Interface = **s1e** |
| 2. Enter the peer IP address at the `(nnn.nnn.nnn.nnn)or address-pool:` prompt. | Peer IP Address = |
| 3. Enter route type **HOST** at the `Route to peer (host/net):` prompt. | Route to Peer= **HOST** |
| **For DSL port 4 (s1f):** | |
| 1. Enter the interface name at the `Input Interface Name:` prompt. | IP Interface = **s1f** |
| 2. Enter the peer IP address at the `(nnn.nnn.nnn.nnn)or address-pool:` prompt. | Peer IP Address = |
| 3. Enter route type **HOST** at the `Route to peer (host/net):` prompt. | Route to Peer= **HOST** |

## Create a Static Route to the NMS

On the Static Routes screen, create a static route to the NMS (on each DSL card).

| Access the . . . | By . . . |
|---|---|
| Static Routes screen | Selecting *Configuration* → *IP Router* → *Static Routes* from the HotWire – DSL menu. |




| **Static Routes Screen** | **A-E-A** |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. Enter **0** or press Return at the `Item Number (0 to add new record):` prompt to add a new record. | |
| 2. Enter the IP address of the NMS at the `Destination (or space to delete route):` prompt. | 1) Host/Net =<br>2) Host/Net =<br>3) Host/Net =<br>4) Host/Net =<br>5) Host/Net =<br>6) Host/Net =<br>7) Host/Net =<br>8) Host/Net =<br>9) Host/Net =<br>10) Host/Net =<br>11) Host/Net =<br>12) Host/Net = |

| **Static Routes Screen** | **A-E-A** |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 3. Do *one* of the following at the `Subnet:(nnn.nnn.nnn.nnn):` prompt:<br>– Enter **255.255.255.255** if you want to create a host route to the IP address specified in Step 2, or<br>– Enter the appropriate subnet mask if you want to enter a network or subnet route. | 1) Subnet Mask =<br>2) Subnet Mask =<br>3) Subnet Mask =<br>4) Subnet Mask =<br>5) Subnet Mask =<br>6) Subnet Mask =<br>7) Subnet Mask =<br>8) Subnet Mask =<br>9) Subnet Mask =<br>10) Subnet Mask =<br>11) Subnet Mask =<br>12) Subnet Mask = |
| 4. Enter the backplane IP address of the MCC card (s1b) at the Next Hop `IP Address (nnn.nnn.nnn.nnn):` prompt. | Next Hop = |
| 5. Enter **1** at the `Input Number:` prompt to specify the preference for this route.<br>1 has the highest preference. The greater the number the lower the preference. | Pref= **1** |
| Up to 12 Network Management Systems (NMSs) can be specified per DSL card. | |

# Customer Domain Configuration Worksheets

For the customer domain, select the DSL card you want to configure, and then configure the following for each of the DSL cards in the HotWire DSLAM:

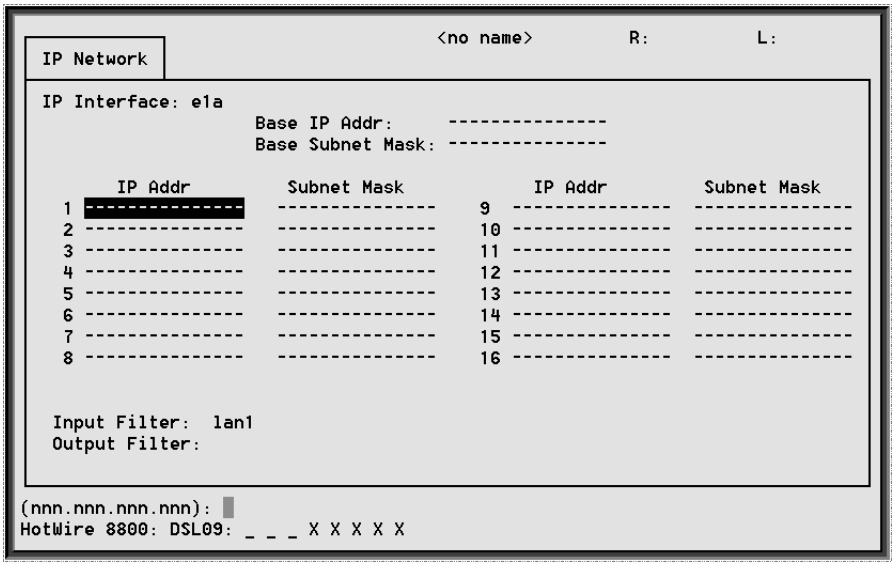
| **Perform this task . . .** | **On this screen . . .** | **To access screen . . .** |
|---|---|---|
| 1. Assign IP addresses to the DSL card LAN interface (e1a). | (HotWire – DSL) IP Network screen | From the HotWire – DSL menu, select: *Configuration → Interfaces → IP Network* |
| 2. Create static routes to end-system users on each DSL card. | (HotWire – DSL) Static Routes screen | From the HotWire – DSL menu, select: *Configuration → IP Router → Static Routes* |
| 3. Create default route. | (HotWire – DSL) Static Routes screen | From the HotWire – DSL menu, select: *Configuration → IP Router → Static Routes* |
| 4. Reset the DSL card. | (HotWire – DSL) Card Reset screen | From the HotWire – DSL menu, select: *Configuration → Card Status → Card Reset* |

Use the worksheets in the following sections to record your network configuration settings. Photocopy the worksheets as needed.

## Assign IP Addresses to the DSL Card LAN

On the IP Network screen, assign IP addresses to the DSL card LAN. Up to 16 ISP domains can be supported per DSL card.

| Access the . . . | By . . . |
|---|---|
| IP Network screen | Selecting *Configuration* → *Interfaces* → *IP Network* from the HotWire – DSL menu. |



| **IP Network Screen** | **A-C-B** |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. Enter the interface name at the `Input Interface Name:` prompt. | IP Interface = **e1a** |
| 2. Enter the IP address at the `(nnn.nnn.nnn.nnn):` prompt.<br>This address must be different than the management domain IP address. | 1) IP Addr =<br>2) IP Addr =<br>3) IP Addr =<br>4) IP Addr =<br>5) IP Addr =<br>6) IP Addr =<br>7) IP Addr =<br>8) IP Addr =<br>9) IP Addr =<br>10) IP Addr =<br>11) IP Addr =<br>12) IP Addr =<br>13) IP Addr =<br>14) IP Addr =<br>15) IP Addr =<br>16) IP Addr = |
| 3. Enter the subnet mask at the `(nnn.nnn.nnn.nnn):` prompt. | 1) Subnet Mask =<br>2) Subnet Mask =<br>3) Subnet Mask =<br>4) Subnet Mask =<br>5) Subnet Mask =<br>6) Subnet Mask =<br>7) Subnet Mask =<br>8) Subnet Mask =<br>9) Subnet Mask =<br>10) Subnet Mask =<br>11) Subnet Mask =<br>12) Subnet Mask =<br>13) Subnet Mask =<br>14) Subnet Mask =<br>15) Subnet Mask =<br>16) Subnet Mask = |
| Up to 16 IP addresses and subnet masks can be entered. Enter the IP addresses and subnet masks for each ISP domain supported by the specified DSL card. | |

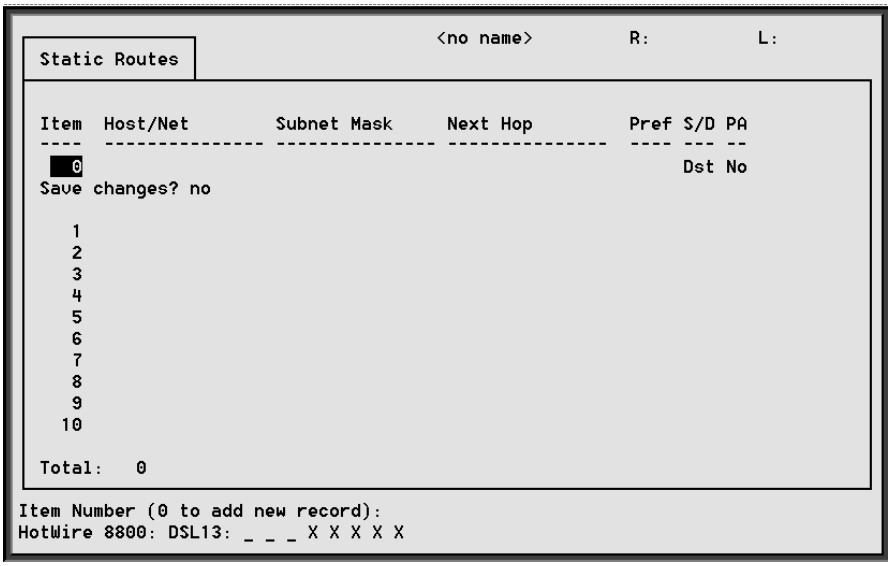
## Create Static Routes to End-User Systems

On the Static Routes screen, create a static route to end-user systems on each DSL card. For host addressing, fill out one worksheet for each end-user system. For structured subnet addressing, complete up to 16 worksheets (up to four worksheets for each of the DSL ports corresponding to the four domains supported on each port).

### NOTE:

Each time you create a static route for an end-user system behind an RTU, you should also create a corresponding source-based input filter rule. See Chapter 7, *IP Filtering*, and Appendix B, *IP Filtering Configuration Worksheets*, for introductory information about the filtering screens. See the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide* for detailed information.

| **Access the . . .** | **By . . .** |
|---|---|
| Static Routes screen | Selecting *Configuration* → *IP Router* → *Static Routes* from the HotWire – DSL menu. |

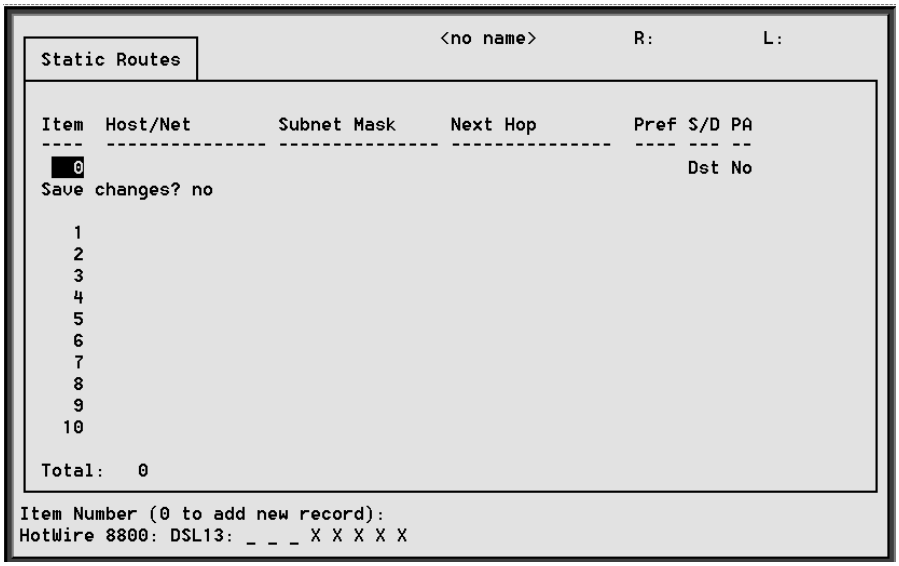


| Static Routes Screen | A-E-A |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. Enter **0** or press Return at the `Item Number (0 to add new record):` prompt to add a new record. | |
| 2. Enter the IP address of the end-user system at the `Destination (or space to delete route):` prompt. | Host/Net = |
| 3. Do *one* of the following at the `Subnet:(nnn.nnn.nnn.nnn):` prompt:<br>– Enter **255.255.255.255** if you want to create a host route to the IP address specified in Step 2, or<br>– Enter the appropriate subnet mask if you want to enter a network or subnet route. | Subnet Mask = |
| 4. Enter the IP address of the associated HotWire 5446 RTU management IP address at the Next Hop `IP Address (nnn.nnn.nnn.nnn):` prompt. | Next Hop = |
| 5. Enter **dst** or **src** at the `Source (Src)/ Destination(dst):` prompt. | S/D= |
| 6. Enter **yes** at the `yes/no:` prompt. | PA= **yes** |
| 7. When the system highlights `Save Changes?`, enter yes at the `yes/no:` prompt. | |

## Create a Default Route or Source Route

On the Static Routes screen, create a default route or source route for each DSL card (upstream direction). If creating a default route, fill out one worksheet. If creating source routing, complete one worksheet per domain (up to 16 domains; four domains per port).

| Access the . . . | By . . . |
|---|---|
| Static Routes screen | Selecting *Configuration* → *IP Router* → *Static Routes* from the HotWire – DSL menu. |

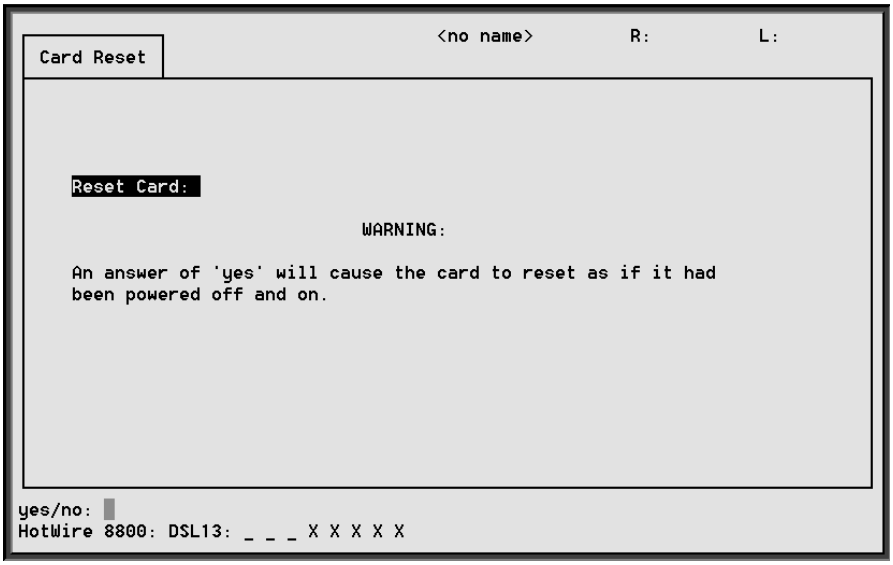



| **Static Routes Screen** | **A-E-A** |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. Enter **0** or press Return at the `Item Number (0 to add new record):` prompt to add a new record. | |
| 2. Do *one* of the following:<br>– To create a default route, enter **0.0.0.0** at the `Destination (or space to delete route):` prompt, or<br>– To create a source route, enter the source route address at the `Destination (or space to delete route):` prompt. | Host/Net = **0.0.0.0** |
| 3. Press RETURN at the `Subnet:(nnn.nnn.nnn.nnn):` prompt. | Subnet Mask = |
| 4. Do *one* of the following:<br>– When creating a default route, enter the IP address of the default route at the Next Hop `IP Address (nnn.nnn.nnn.nnn):` prompt, or<br>– When creating a source route, enter the IP address of the source route at the Next Hop `IP Address (nnn.nnn.nnn.nnn):` prompt. | Next Hop = |

| Static Routes Screen | A-E-A |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 5. Enter **1** at the `Input Number:` prompt to specify the preference for this route.<br>1 has the highest preference. The greater the number the lower the preference. | Pref= **1** |
| 6. Enter **dst** or **src** at the `Source (Src)/ Destination(dst):` prompt. | S/D= |
| 7. Enter **no** or press RETURN at the `yes/no:` prompt to keep the NO value under the PA (proxy ARP) column. | PA= **no** |
| 8. When the system highlights `Save Changes?`, enter yes at the `yes/no:` prompt. | |

## Reset the DSL Card

After configuring the DSL card for the customer domain, reset the card. On the Card Reset screen (*Configuration* → *Card Status* → *Card Reset)*, reset the DSL card by entering **yes** at the `yes/no:` prompt.



# IP Filtering Configuration Worksheets

# B

## Overview

This appendix provides worksheets to assist you in creating filters for your HotWire DSLAM network. Use the worksheets to record filter parameters such as IP filter types and rule types for the MCC card and DSL cards. Photocopy the worksheets as needed. After the worksheets are completed, define the filters and rule types via the HotWire DSLAM user interface.

The worksheets are based on the network model and IP filtering theory described in this guide. For an explanation of the network model and IP filtering theory, review the chapters in this guide. For specific information about the user interface screens and fields, see the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

## Summarizing How to Define a Filter

To define a filter for a specific interface to indicate whether a packet can be forwarded or discarded on that interface:

- Go to the appropriate IP Filter Configuration screen to define a filter and set up one or more rule types (network address rule type, host address rule type, and/or socket address rule type) for that filter.
- Go to the appropriate IP Network screen to bind the filter (i.e., specify the filter type (input filter or output filter) by specifying the name of the filter in the appropriate field and binding it to a specific interface).

**NOTE:**

For each DSL card, the HotWire DSLAM provides the following default filter names:

- **lan1** – bound to e1a
- **dsl1** – bound to DSL port #1
- **dsl2** – bound to DSL port #2
- **dsl3** – bound to DSL port #3
- **dsl4** – bound to DSL port #4

For the MCC card, **lan1** (bound to e1a) is the only default filter.

When using these filter names as input filters, by default, these filters are already bound to their corresponding interfaces. To use these filter names as output filters, you must manually bind them on the IP Network screen.

Keep in mind that up to 33 rules can be configured for each filter. By default, if you do not specify rules, the system will forward packets.

# Filtering Configuration Worksheets

The following sections provide worksheets for configuring filters. Use these worksheets when creating filters on the MCC or DSL cards.

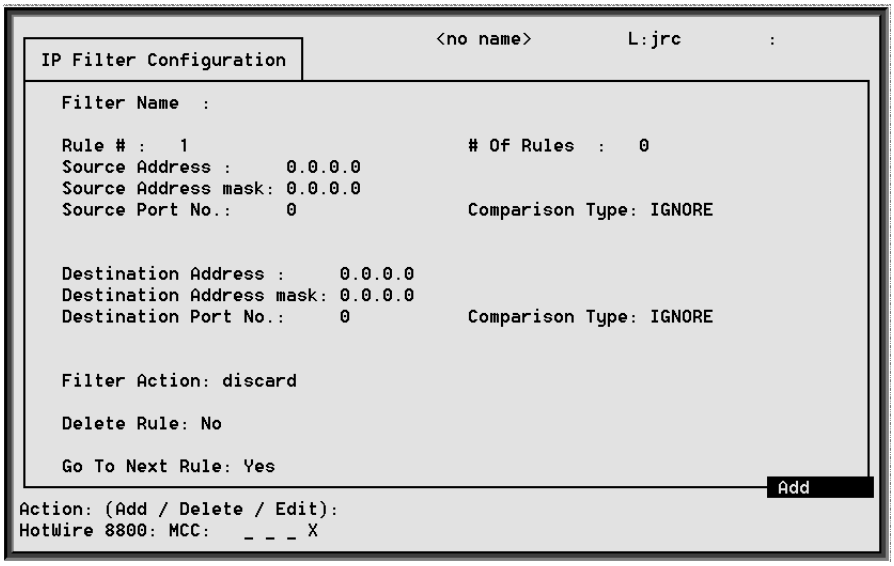
## Defining the Filter and Rules

On the IP Filter Configuration screen, create a filter and define its rules. Complete one worksheet for each rule.

**NOTE:**

In this release, up to 33 rules can be configured for each filter. By default, if you do not specify rules, the system will forward packets.

| Access the . . . | By . . . |
|---|---|
| IP Filter Configuration screen | Selecting *Configuration* → *IP Router* → *IP Router Filters* from the appropriate menu (HotWire – MCC menu or the HotWire – DSL menu). |



| **IP Filter Configuration** | **A-E-C** |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. At the `Action: (Add/Delete/Edit):` prompt, type **A** to add a rule. | |
| 2. Enter the name of the filter for which you want to define rules at the `Enter Filter Name:` prompt.<br>The DSLAM provides the following filter names that are already bound to the appropriate interface:<br>– For the e1a interface, enter **lan1.**<br>– For the DSL port #1 interface, enter **dsl1.**<br>– For the DSL port #2 interface, enter **dsl2.**<br>– For the DSL port #3 interface, enter **dsl3.**<br>– For the DSL port #4 interface, enter **dsl4** .<br><br>NOTE: You can change these default filter names. However, if you change the filter names on this screen, you must remember to change the name specified in the `Input Filter` field on the IP Network screen. If you do not change the default names, you do not need to go to the IP Network screen, because the default filter names are already bound to the appropriate interface. | Filter Name = |

| IP Filter Configuration | A-E-C |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 3. Depending on the rule type (or combination of rule types) you want to define, do one or more of the following:<br>– To define a *network address rule type*, specify either an IP address or subnet mask in the `Source Address` and `Source Address mask` fields, or the `Destination Address` and `Destination Address mask` fields.<br>– To define a *host address rule type*, specify either an IP address or subnet mask in the `Source Address` and `Source Address mask` fields, or the `Destination Address` and `Destination Address mask` fields.<br>– To define a *socket address rule type*, specify the source (socket) port number at the `Source Port No.` field and the destination (socket) port number at the `Destination Port No.` field. This rule type may be used in conjunction with a network address or host address rule type.<br>If defining a socket address rule type, you must also specify the comparison type you want to perform in the Comparison Type field. Enter **IGNORE** if you do not want to do a comparison, or one of the following to do a comparison on the port number specified in the packet and the rule: **EQ** (equal to), **NEQ** (not equal to), **GT** (greater than), **LT** (less than), **IN_RANGE** (within the specified range), **OUT_RANGE** (outside of the specified range).<br>For a description of these rule types, see Chapter 7, *IP Filtering*. | **Rule #** ____<br>Source Address =<br>Source Address mask =<br>Source Port No. =<br>Comparison Type =<br><br>Destination Address =<br>Destination Address mask =<br>Destination Port No. =<br>Comparison Type = |
| 4. Enter **filter** at the `Filter Action:` prompt to activate filtering for the specified filter name, or **discard** to prevent packets that match the rule(s) from passing through. | Filter Action = |

## Binding the Filter

On the IP Network screen, indicate whether you want to use the filter you have just defined on the IP Filter Configuration screen as an input filter or an output filter for a specific interface on the MCC or DSL card.

### NOTE:

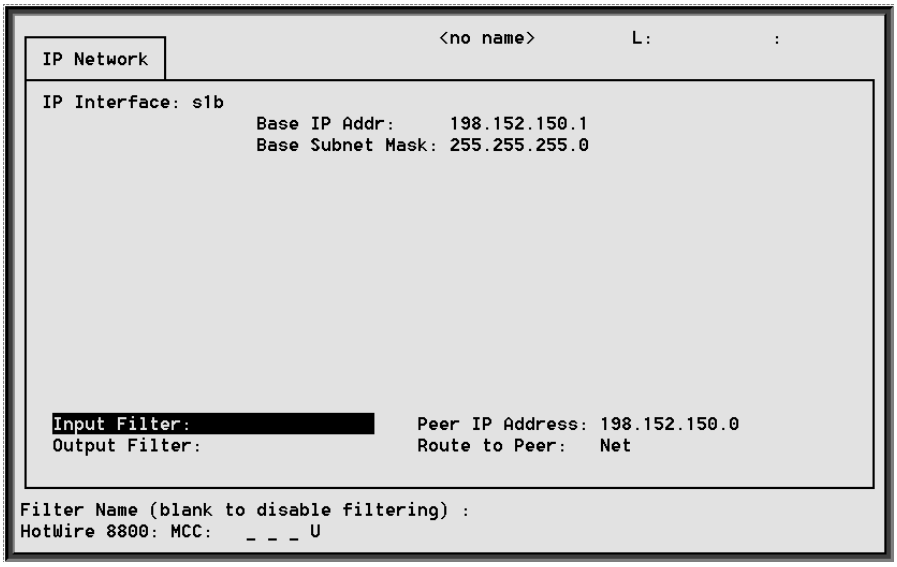
When using the default input filter names, you do not need to complete a worksheet. The default filter names are already bound to their corresponding interfaces, and no further action needs to be done.

However, you will need to complete the following worksheet if you:

— Changed the default input filter name(s) on the IP Filter Configuration screen, or

— Defined an output filter and that filter needs to be bound to a specific interface

| Access the . . . | By . . . |
|---|---|
| IP Network screen | Selecting *Configuration* → *Interfaces* → *IP Network* from the appropriate menu (HotWire – MCC menu or the HotWire – DSL menu). |



| **IP Network Screen** | **A-C-B** |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. Enter the interface name at the `Input Interface Name:` prompt. | IP Interface = **s1b** |
| 2. Enter *one* of the following:<br>– For the Input Filter field, enter the desired filter name at the `Filter Name (blank to disable filtering):` prompt.<br>Use an input filter to prevent packets entering the DSL card through a specified interface from being forwarded.<br>– For the Output Filter field, enter the desired filter name at the `Filter Name (blank to disable filtering):` prompt.<br>Use an output filter to prevent packets from going out of the DSL card through a specified interface. | Input Filter =<br>or<br>Output Filter =<br>NOTE: You can specify an input filter for one interface and an output filter for another interface. Do not, however, specify an input filter and an output filter for the same interface.<br>Remember, if you are using the default filter names as input filters, the filters are already bound to their corresponding interface. |

# SNMP Configuration Worksheets

# C

## Overview

This appendix provides worksheets to assist you in setting up general SNMP configurations for your HotWire DSLAM network, such as defining communities, enabling traps, and preventing unauthorized access to the DSLAM. Use the worksheets (when configuring both MCC and DSL cards) to record SNMP configuration parameters such as community names and IP addresses for associated SNMP NMS managers for a specific card. After the worksheets are completed, configure the SNMP agent via the HotWire DSLAM user interface.

The worksheets are based on the network model and SNMP agent configuration theory described in this guide. For an explanation of the network model and SNMP agent configuration theory, review the chapters in this guide. For specific information about the user interface screens and fields, see the *HotWire Digital Subscriber Line Access Multiplexer (DSLAM) User's Guide*.

## Summarizing the General SNMP Agent Configuration

In summary, to configure the SNMP agent:

- On the SNMP Communities/Traps screen, do the following:
  - — Assign an SNMP NMS manager to a community by specifying the SNMP NMS manager's IP address to a community name.
  - — Configure the generation of all trap messages (except for the Authentication Failure Trap messages, which can be enabled or disabled independently).
  - — Enable or disable the generation of Authentication Failure trap messages.
- On the SNMP Security screen, you can enter the IP addresses of specific, approved SNMP NMS managers to prevent other managers from browsing the HotWire DSLAM network. Use this screen to prevent unauthorized access to the DSLAM.

# SNMP Agent Configuration Worksheets

The following sections provide worksheets for configuring the SNMP agent. Use these worksheets when preparing SNMP configuration on both the MCC and DSL cards.

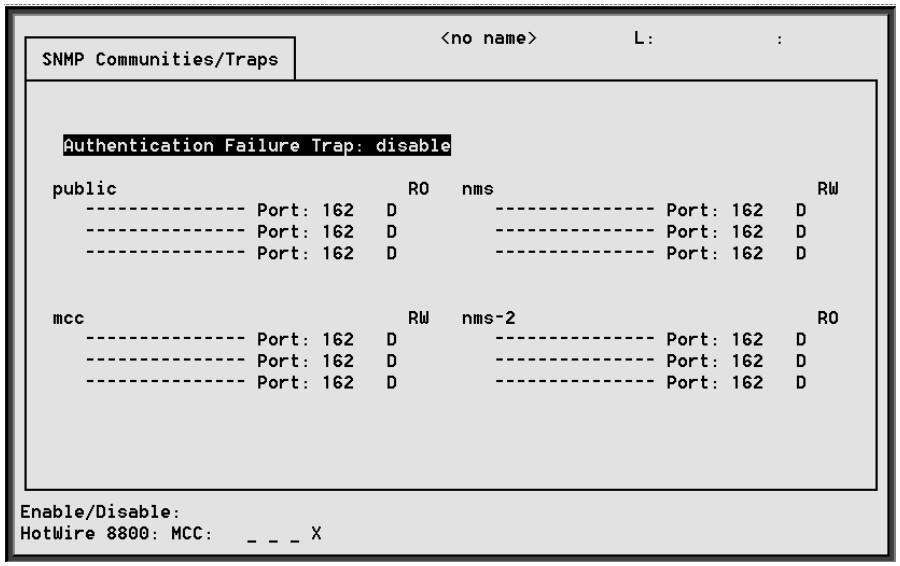
## Defining a Community and Enabling Traps

On the SNMP Communities/Traps screen, define a community by specifying the SNMP NMS manager who will receive traps and who has permission to browse. Up to three managers can be assigned for each community. Also, on this screen, you can enable or disable the generation of traps.

| **Access the . . .** | **By . . .** |
|---|---|
| SNMP Communities/Traps screen | Selecting *Configuration* → *SNMP* → *Communities/Traps* (**A-F-D**) from the HotWire – MCC menu if configuring the MCC card.<br><br>Selecting *Configuration* → *SNMP*→*Communities/Traps* (**A-F-C**) from the HotWire – DSL menu if configuring a DSL card. |

### NOTE:

The following screen is the SNMP Communities/Traps screen from the HotWire – MCC menu. The SNMP Communities/Traps screen from the HotWire – DSL menu is not shown. However, it displays the same fields and prompts.



| SNMP Communities/Traps | |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. Determine whether you want to enable or disable Authentication Failure traps:<br>– Enter **enable** at the `Enable/Disable:` prompt to forward authentication failure traps to all SNMP NMS managers assigned to a community name.<br>– Enter **disable** at the `Enable/Disable:` prompt to prevent the forwarding of authentication failure traps to all SNMP NMS managers assigned to a community name. | Authentication Failure Trap = |
| 2. Change the default community names at the `Community Name:` prompt if desired. HotWire DSLAM provides the following default community names:<br>– **public** (RO – Read Only)<br>– **mcc** (RW – Read Write)<br>– **nms** (RW – Read Only)<br>– **nms - 2** (RO – Read Write)<br><br>You can also change the access permission for these communities. At the `ReadOnly (ro)/ReadWrite (rw)/NoAccess (na):` prompt, specify the desired permission for each community.<br><br>NOTE: Make sure the SNMP NMS manager knows the correct community name. It will need the correct community name to access/browse the HotWire DSLAM. | Record the Community Names (default or new names) and their access permissions.<br>**public** or _____<br>Access permission =<br>**mcc** or _____<br>Access permission =<br>**nms** or _____<br>Access permission =<br>**nms – 2** or _____<br>Access permission = |

| SNMP Communities/Traps | |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 3. For each community name, you can enter IP addresses of up to three SNMP NMS managers.<br>– At the `(nnn.nnn.nnn.nnn):` prompt, enter the IP addresses of the SNMP NMS managers.<br>– At the `Input Number:` prompt, enter the port number for each SNMP NMS manager specified.<br>– At the `Enable/Disable:` prompt, indicate whether or not you want to enable or disable the generation of traps. Enter **E** to enable traps. This will forward traps to the specified SNMP NMS manager. Enter **D** to disable traps. This prevents the forwarding of traps. | **public** (RO) or _____:<br>■ IP address =<br>Port =<br>Forward traps (E or D) =<br>■ IP address =<br>Port =<br>Forward traps (E or D) =<br>■ IP address =<br>Port =<br>Forward traps (E or D) =<br>**mcc** (RW) or _____:<br>■ IP address =<br>Port =<br>Forward traps (E or D) =<br>■ IP address =<br>Port =<br>Forward traps (E or D) =<br>■ IP address =<br>Port =<br>Forward traps (E or D) =<br>**nms** (RW) or _____:<br>■ IP address =<br>Port =<br>Forward traps (E or D) =<br>■ IP address =<br>Port =<br>Forward traps (E or D) =<br>■ IP address =<br>Port =<br>Forward traps (E or D) =<br>**nms – 2** (RO) or _____:<br>■ IP address =<br>Port =<br>Forward traps (E or D) =<br>■ IP address =<br>Port =<br>Forward traps (E or D) =<br>■ IP address =<br>Port =<br>Forward traps (E or D) = |

## Preventing Unauthorized Access

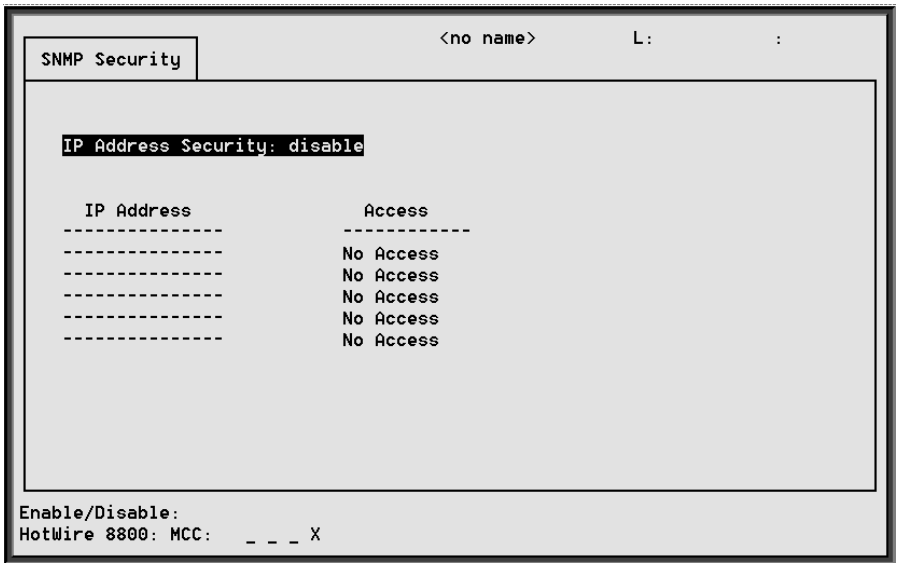
Use the SNMP Security screen to enable SNMP security (i.e., prevent unauthorized managers from browsing the HotWire DSLAM network).

- If address security is to be activated, it should be activated on the MCC and all DSL cards.
- If the NSP wants to allow an ISP or customer access to a limited set of DSL cards, that NMS's IP address should only be entered on the MCC and those DSL cards in the limited set.

| **Access the . . .** | **By . . .** |
|---|---|
| SNMP Security screen | Selecting *Configuration* → *SNMP* → *Security* (**A-F-A**) from the HotWire – MCC menu if configuring the MCC card.<br><br>Selecting *Configuration* → *SNMP* → *Security* (**A-F-A**) from the HotWire – DSL menu if configuring a DSL card. |

### NOTE:

The following screen is the SNMP Security screen from the HotWire – MCC menu. The SNMP Security screen from the HotWire – DSL menu is not shown. However, it displays the same fields and prompts.



| SNMP Security | |
|---|---|
| **Prompt** | **Your Configuration Setting** |
| 1. Determine whether you want to enable or disable IP address security:<br>– Enter **enable** at the `Enable/Disable:` prompt to enable (turn on) security.<br>– Enter **disable** at the `Enable/Disable:` prompt to disable (turn off) security. | IP Address Security = |
| 2. At the `(nnn.nnn.nnn.nnn)` prompt, enter the IP address of an SNMP NMS manager(s).<br>For each manager, specify the access permission: **NA** (No Access), **RO** (Read Only), or **RW** (Read Write).<br>NOTE: You can enter up to five SNMP NMS managers. | ■ IP Address =<br>Access =<br>■ IP Address =<br>Access =<br>■ IP Address =<br>Access =<br>■ IP Address =<br>Access =<br>■ IP Address =<br>Access = |

# Glossary

**10BaseT** The technical term for twisted-pair Ethernet.

**Address Mask** *See* Subnet Address Mask.

**ARP** Address Resolution Protocol. The TCP/IP protocol used to dynamically bind an IP address to a low-level physical hardware address (usually a Media Access Control (MAC) address).

**ATM** Asynchronous Transfer Mode. Cell-switching rather than frame relay technology.

**BootP** BOOTstrap Protocol. A protocol the MCC card uses to obtain startup information, including IP address from the DSL cards.

**CAP** Carrierless Amplitude Modulation/Phase Modulation. A transmission technology for implementing a Digital Subscriber Line (DSL). The transmit and receive signals are modulated into two wide-frequency bands using pass band modulation techniques.

**DCE Manager** A network management system that helps the network administrator manage devices using Simple Network Management Protocol (SNMP).

**Default Route** An IP address specified as 0.0.0.0.

**Domain** A block of IP addresses. Syntactically, all IP addresses within a given domain would share a common IP address prefix of some length.

**DSL Card** Digital Subscriber Line Card. The primary card in the HotWire DSLAM system. It has one Ethernet port and four DSL ports.

**DSLAM** HotWire 8600 or 8800 Digital Subscriber Line Access Multiplexer.

**e1a** Name of the DSL card's and MCC card's 10BaseT interface.

**end-user system (ES)** Any end-user computer system that connects to a network.

**Filter** A rule or set of rules applied to a specific interface to indicate whether a packet can be forwarded or discarded.

**HDLC** High-level Data Link Control protocol.

**Host** *See* end-user system (ES).

**Host Routes** A host having a subnet mask of 255.255.255.255.

**Hub** An electronic device to which multiple computers attach, usually using twisted-pair wiring.

**ICMP** Internet Control Management Protocol. An Internet protocol that allows for the generation of error messages, test packets, and information messages related to IP.

**Internet** A collection of networks and routers using TCP/IP protocols to form a single cooperative virtual network.

**IP** Internet Protocol. The TCP/IP standard protocol that defines the IP datagram as the unit of information passed across an Internet and provides the basis for connectionless, best-effort packet delivery service.

**IP Address** Internet Protocol Address. This is a 32-bit address assigned to a host on a TCP/IP Internet. The IP address has a host component and a network component.

| | |
|---|---|
| **ISDN** | Integrated Services Digital Network. |
| **ISP** | Internet Service Provider. |
| **LAN** | Local Area Network. Any physical network technology designed to span short distances. |
| **MAC Address** | Media Access Control Address. Areas of memory your CPU uses to distinguish between the various peripheral devices connected to your system when transferring or receiving data. The MAC address is also known as the physical address. |
| **MCC Card** | Management Communications Controller Card. The card in a HotWire DSLAM system or stack that is used primarily for monitoring and configuring the HotWire DSLAM. |
| **MIB** | Management Information Base. A collection of information (e.g., configuration, status, and statistical data) within an SNMP agent that forms a database of information about the agent which is accessible from the NMS manager. MIB II is the current standard. |
| **multihomed system** | A system with connections to two or more logical networks, which may be assigned to one or more physical networks. |
| **NAP** | Network Access Provider. The NAP provides a transit network service permitting connection of service subscribers to Network Service Providers (NSPs). The NAP is typically the network provider (e.g., a Regional Bell Operating Company, an Alternate Local Exchange Carrier) that has access to the copper twisted pairs over which the DSLs operate. |
| **NID** | Network Interface Device. An electronic device that connects the telephone line and POTS splitter to the telephone network. |
| **NMS** | Network Management System. An NMS communicates to a Simple Network Management Protocol (SNMP) agent via SNMP to obtain (get) or configure (set) specific parameters or variables within control of the SNMP agent (e.g., DCE Manager). |
| **NSP** | Network Service Provider. NSPs can be either public data network providers (i.e., Internet Service Providers) or private data network providers (i.e., corporate intranets) who provide network services based on the Internet Protocol (IP). In some cases, the NSP and the NAP can be a single network provider. |
| **Packet** | Used in this document to refer to a block of data sent across an IP switching network. |
| **Ping** | An IP-based application used to test reachability of destinations by sending an ICMP echo request and waiting for a reply. The ping program is supported from both the DSL and MCC cards. |
| **POP** | Point of Presence. The POP is the access point to the Network Access Provider network for a Network Service Provider (NSP). The NSP is typically connected to the POP across an access link that terminates on a router on the NSP premises. |
| **POTS** | Plain Old Telephone Service. |
| **POTS Splitter** | A device that filters out the DSL signal and allows the POTS frequencies to pass through. This device can be installed at the Central Office or Customer Premises. |
| **PPP** | Point-to-Point Protocol. A protocol for framing IP when sending across a serial line. |
| **Proxy ARP** | Proxy Address Resolution Protocol (ARP). The technique in which one machine, usually a router, answers ARP requests intended for another by supplying its own physical address. By pretending to be another machine, the router accepts responsibility for forwarding packets. The purpose of proxy ARP is to allow a site to use a single IP network address with multiple physical networks. |
| **RADSL** | Rate Adaptive Digital Subscriber Line. |
| **Router** | A special purpose, dedicated computer that attaches to two or more networks and forwards packets from one to the other. |

| | |
|---|---|
| **Routing Table** | A table that stores information about possible destinations for packets being routed through the HotWire DSLAM and identifies the next hop address to which to send the packet. |
| **RTU** | Remote Termination Unit. A device, such as the HotWire 5446 RTU, that is installed at the end-user site (or customer premises). The RTU connects to the local loop to provide high-speed Internet or Intranet connectivity to the HotWire DSLAM. |
| **s1b** | Interface name of the card's interface to the DSLAM system backplane bus. |
| **s1c** | Interface name of a DSL card's DSL port #1. |
| **s1d** | Interface name of a DSL card's DSL port #2. |
| **s1e** | Interface name of a DSL card's DSL port #3. |
| **s1f** | Interface name of a DSL card's DSL port #4. |
| **Service Subscriber** | The service subscriber is the user (or set of users) that has contracted to receive networking services (e.g., Intranet access, remote LAN access) from one or more Network Service Providers (NSPs). |
| **SNMP** | Simple Network Management Protocol. An application-level protocol used in network management. |
| **SNMP Agent** | An application level program typically running on a host system which facilitates communication to an NMS manager. *See* NMS. |
| **SNMP Trap** | A notification message to the SNMP manager when an unusual event occurs on a network device, such as a reinitialization. |
| **Source-Based Routing** | A security feature for preventing end-user system to end-user system routing when the end-user systems are attached to LANs on different RTUs (that are attached to the same DSL card). That is, sourced-based routing can ensure that all upstream traffic within a customer domain is sent to the ISP. |
| **Static Route** | A permanent entry into the routing table that is manually entered. |
| **Subnet Address Mask** | A bit mask used to select bits from an IP address for subnet addressing. The mask is 32 bits long and selects the network portion of the IP address and one or more bits of the local portion. |
| **TCP** | Transmission Control Protocol. The TCP/IP standard transport level protocol that provides the reliable, full-duplex, stream service on which many application protocols depend. |
| **Telnet** | A simple remote terminal protocol that is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. Telnet allows the user of one host computer to log into a remote host computer, and interact as a normal terminal user for that host. |
| **tFTP** | Trivial File Transfer Protocol. |
| **Traceroute** | A program that prints the path to a destination. |
| **VLAN** | Virtual Local Area Network. |
| **VLAN Switch** | A layer 2 networking device. |
| **WAN** | Wide Area Network. |
| **WAN-C** | Wide Area Network Concentrator. The WAN-C concentrates data traffic from one or more DSLAMs onto facilities providing access to the WAN. The WAN-C can be either a router (a layer 3 networking device) or a VLAN switch (a layer 2 networking device). |
| **Wiring center** | A wiring center is usually a local serving office where the DSLs from the service subscribers are terminated on the HotWire DSLAM. |

# Index

## Numbers


10BaseT interface on the MCC and DSL cards (e1a), 5-1
5446 RTU
  configuring the management domain IP addresses, A-10
  description, 1-5
  proxy ARP, 4-4
8600 DSLAM, 1-2
8800 DSLAM, 1-3


## A


address allocation schemes
  host addressing, 5-2
  structured subnet addressing, 5-3
Address Resolution Protocol (ARP), 1-9
address types in routing table, 6-1
applications for management
  ping, 3-2
  telnet, 3-3
  tFTP client, 3-3
assigning
  an IP address to the backplane (s1b), A-4
  an IP address to the MCC card, A-2
  IP addresses to the DSL cards, A-5, A-15
assigning IP addresses
  for the customer domain, 5-9
  for the management domain, 5-6
Asynchronous Transfer Mode (ATM), 1-9
audience, v


## B


binding a filter, B-6


## C


chassis types
  HotWire 8600 DSLAM, 1-2
  HotWire 8800 DSLAM, 1-3
circuit cards
  DSL card, 1-4
  MCC card, 1-4
Components of the DSLAM
  chassis, 1-2
  DSL card, 1-4
  MCC card, 1-4
configuration of the SNMP agent, 8-3
configuration worksheets
  filtering configuration, B-1
  mandatory network configuration, A-1
  SNMP configuration, C-1
configuring the RTU management domain IP addresses, A-10
creating
  a default route (management domain), A-7
  a default route or source route (customer domain), A-18
  a static route to the NMS, A-11
  static routes to end–user systems, A-17
customer domain
  assigning IP addresses to the DSL cards, A-15
  components, 4-1
  configuration worksheets, A-14
  creating a default route or source route, A-18
  creating static routes to end–user systems, A-17
  DSL card proxy ARP, 4-3
  HotWire 5446 RTU proxy ARP, 4-4
  IP address allocation, 5-9
  packet walk–through, 9-1
  resetting the DSL card, A-20
  using a filter, 7-3
customer domain features
  data rates, 2-1
  filtering, 2-5
  protocols, 2-2
  proxy ARP, 2-3


## D


DCE Manager, 3-1, 8-1
default route, 6-2, A-7, A-18
defining
  a community, C-2
  a filter, B-3

destination–based routing, 6-1
directed broadcasts, 2-2
discovering devices on the network, 4-6
discovery, 4-6
document
  purpose, v
  summary, vi
domain types, 1-11
DSL card
  assigning IP addresses, A-15
  assigning IP addresses to the DSL cards, A-5
  description, 1-4
  proxy ARP, 4-3
  resetting the card, A-20
  static route example, 6-4
DSL ports (s1c, s1d, s1e, and s1f)
  naming convention of ports on the DSL card, 5-1
  setting the peer IP address, 5-7
DSLAM
  components, 1-2
  description, 1-1
  overview of the network model, 1-7
  supported MIBs, 8-2
  system backplane interface (s1b), 5-1, 5-7

## E

e1a, 5-1
enabling SNMP traps, C-2

## F

filter
  binding a filter, B-6
  configuration worksheets, B-1
  defining a filter and rules, B-3
  description, 7-1
  rule types, 7-2
  security advantages, 7-3
  service security scenario, 7-4
  types of filters, 7-1

## H

High level Data Link Control (HDLC), 2-2
host address rule type, 7-2
host addressing, 5-2
host route address, 6-1
HotWire devices
  5446 RTU, 1-5
  8600 DSLAM, 1-2
  8800 DSLAM, 1-3
  DSL card, 1-4
  MCC card, 1-4

## I

input filter, 7-1
interface naming convention, 5-1
Internet Control Management Protocol (ICMP), 2-2
Internet Protocol (IP), 2-2
IP address allocation schemes
  host addressing, 5-2
  structured subnet addressing, 5-3

## M

MAC, 2-2
MAC address, 1-9
management domain
  assigning an IP address to the MCC card, A-2
  assigning IP address to the backplane (s1b), A-4
  assigning IP addresses to the DSL cards, A-5
  components, 4-5
  configuration worksheets, A-2
  configuring the RTU management domain IP addresses, A-10
  creating a default route, A-7
  creating a static route to the NMS, A-11
  discovering devices on the network, 4-6
  IP address allocation, 5-6
  MCC card proxy ARP, 4-7
  packet walk–through, 9-3
  peer IP addresses, 5-7
  resetting the MCC card, A-9
  using a filter, 7-3
management domain features
  network management, 3-1
  ping, 3-2
  Telnet, 3-3

tFTP client, 3-3
MCC card
assigning an IP address to the MCC card, A-2
description, 1-4
proxy ARP, 4-7
resetting the card, A-9
static route example, 6-3
MIB compliance, 8-1
multicasting, 2-2

## N

Network Access Provider (NAP), 1-8
network address rule type, 7-2
network configuration worksheets, A-1
Network Management System (NMS), 8-1
network model
customer domain components, 4-1
discovering devices on the network, 4-6
domain types, 1-11
management domain components, 4-5
network model
Network Access Provider (NAP), 1-8
Network Service Provider (NSP), 1-9
overview, 1-7
service subscriber, 1-8
network route address, 6-1
Network Service Provider (NSP), 1-9

## O

organization of document, vi
output filter, 7-1

## P

peer IP addresses, 5-7
ping program, 3-2
Point–of–Presence (POP), 1-9
Point–to–Point Protocol (PPP), 2-2
port naming convention, 5-1
POTS splitter, 1-1, 1-5
preventing unauthorized access, C-5
preventing unwanted traffic from leaking, 7-3
product–related documents, vii
proxy ARP, 2-3, 4-3, 4-7

## R

recording your configuration settings, 5-10
regional center, 1-9
related documents, vii
Remote Termination Unit (RTU)
configuring the management domain IP addresses, A-10
description, 1-5
proxy ARP, 4-4
resetting
the DSL card, A-20
the MCC card, A-9
routing
destination–based, 6-1
source–based, 6-5
routing table
description, 6-1
types of addresses, 6-1
rule types
host address, 7-2
network address, 7-2
socket address, 7-2

## S

s1b, 5-1, 5-7, A-4
service security filtering scenario, 7-4
service subscriber, 1-8
setting the peer IP addresses, 5-7
Simple Network Management Protocol (SNMP), 8-1
SNMP agent
defining a community, C-2
enabling traps, C-2
general configuration, 8-3
overview, 8-1
preventing unauthorized access, C-5
summarizing the configuration, C-1
SNMP configuration worksheets, C-1
SNMP traps, 8-2, C-2
socket address rule type, 7-2
source route, A-18
source–based routing, 6-5
spoofing, 7-3
static route examples
DSL card static route, 6-4
MCC card static route, 6-3

static routes, 6-1, A-17
structured subnet addressing, 5-3
subnet broadcasts, 2-2
subnet route address, 6-1
summarizing
  filter configuration, B-1
  general SNMP agent configuration, C-1
  network configuration, A-1
summary of document, vi
supported MIBs, 8-2
system backplane interface (s1b), 5-1, 5-7

## T

telnet, 3-3
tFTP client, 3-3

## U

using a filter for security advantages, 7-3

## V

VLAN switch, 1-10

## W

Wide Area Network (WAN), 1-9
Wide Area Network concentrator (WAN–C), 1-9
wiring center, 1-9